Úvod do teorie množin

Poznámky z předmětu **NAIL063** doc. Kynčla

Letní semestr 2023/2024

Jakub Smolík

Obsah

1 Cantorova naivní teorie množin

Naivní teorií myslíme teorii, která nemá formálně dané axiomy. Místo toho se na její popis používá přirozený jazyk. Na množiny pohlíží jako na soubory libovolných „věcí". Tento přístup je intuitivní a ve většině případů zcela dostačující. Běžně v matematice pracujeme s množinami tímto způsobem a ničemu to nevadí. Ale ukáže se, že to vede k celé řadě paradoxů.

Sám Cantor si byl například vědom toho, že jeho teorie připouští existenci množiny všech množin, přestože z Cantorovy věty vyplývá, že množina všech množin neexistuje. Tento paradox ale nebyl natolik zásadní, aby donutil Cantora přehodnotit svoji teorii.

Pravděpodobně ten nejdůležitější paradox, který nadobro pohřbil Cantorovu naivní teorii a dal vzniknout axiomatickým teoriím množin, byl Russelův paradox.

1.1 Russelův paradox

Jako první ho zřejmě objevil matematik Ernst Zermelo roku 1899, ale své zjištění nezveřejnil. Publikoval ho až Russell v roce 1901. Návrh první teorie, která se tomuto paradoxu snažila vyhnout, přišel od Zermela v roce 1908. Matematik Abraham Fraenkel ovšem roku 1921 poukázal na to, že v Zermelově teorii není možné dokázat existenci některých množin, jejichž existenci většina tehdejších množinových teoretiků považovala za samozřejmou. Následující rok navrhl úpravu axiomů této teorie, čímž vznikla dnes velmi rozšířená Zermelo-Fraenkelova teorie množin (ZF). Velmi hezké video o Russelově paradoxu je ZDE.

Definice. Množina M je krotká $\equiv M \notin M$; jinak je divoká.

Například *množina všech zvířat* je krotká, zatímco *množina všech věcí, které nejsou čajové lžičky* je divoká. Zajímavá je třeba *množina všech věcí, na které právě myslím.* Většinou je krotká, ale právě teď, když píšu tuto větu, je divoká.

Podívejme se na množinu všech krotkých množin $M := \{x \mid x \text{ je krotká}\}$. Je krotká, nebo divoká? Pokud je krotká, potom splňuje definiční podmínku M, tedy $M \in M$, takže je divoká. Pokud je divoká, potom nesplňuje definiční podmínku M, tedy $M \notin M$, takže je krotká. Čili je krotká $\iff$ je divoká.

Russelův paradox nám ukazuje, že musíme nějak omezit, co vše může být množinou.

1.2 Berryho paradox

Berryho paradox naopak ukazuje, že definice pomocí přirozeného jazyka mohou vést k paradoxům. Proto se budeme snažit věci definovat jazykem matematické logiky.

Paradox zní takto: Označme m nejmenší přirozené číslo, které nelze definovat méně než sto písmeny.

Anglická abeceda + mezera = 27 znaků, takže celkem 27^{100} kombinací, tedy takovéto m existuje. Víme, že m nelze definovat, ale věta výše (která má určitě méně než 100 znaků) ho definuje.

2 Nejprve trochu logiky

2.1 Jazyk teorie množin

Jazyk teorie množin je $\langle \in \rangle$ s rovností, kde $\in$ je binární relační symbol. Mohli bychom uvažovat i jazyk bez rovnosti a přidat nový binární relační symbol '=' a axiomy rovnosti. V každém jazyku je implicitně

- spočetně mnoho symbolů pro proměnné: $x_1, x_2, x_3, \dots$,
- pro každou proměnnou x dva symboly s kvantifikátory: $(\forall x)$, $(\exists x)$,
- symboly pro logické spojky: $\wedge, \vee, \implies, \iff$,
- čárka a závorky.

Tento jazyk ještě rozšíříme několik zkratek. Konkrétně definujme

- $x \neq y \equiv \neg x = y$,
- $x \notin y \equiv \neg x \in y$,
- $x \subseteq y \equiv (\forall z)(z \in x \Rightarrow z \in y)$,
- $x \subset y \equiv x \subseteq y \wedge x \neq y$.

2.2 Termy a formule

Nyní uvažujme obecný jazyk L s množinou relačním symbolů $\mathcal{R}$ a množinou funkčních symbolů $\mathcal{F}$. Konstantní symboly jsou funkční symboly arity nula.

Definice 1. Termy jazyka L jsou konečné nápisy definované induktivně:

- každá proměnná a každý konstantní symbol z L je term,
- pro funkční symbol f arity n a termy $t_1, \dots t_n$ je term i nápis $f(t_1, \dots t_n)$.

Definice 2. Atomická formule je nápis $R(t_1, \dots t_n)$, kde R je n-ární relační symbol a t_i jsou termy.

Definice 3. Formule jazyka L jsou konečné nápisy definované induktivně:

- každá atomická formule jazyka L je formule,
- jsou-li φ a ψ formule, potom jsou formule i nápisy

$$(\neg\varphi), (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \Rightarrow \psi), (\varphi \Leftrightarrow \psi), ((\forall x)\varphi), ((\exists x)\varphi).$$

Formule mají přirozenou stromovou strukturu. Výskyt proměnné x je list tohoto stromu označený x. Podformule jsou podstromy tohoto stromu.

Definice 4 (Volné a vázané proměnné)**.** Výskyt proměnné x ve formuli φ je

- vázaný $\equiv$ vyskytuje se v nějaké podformuli začínající $(\forall x)$ nebo $(\exists x)$,
- volný $\equiv$ není vázaný.

Proměnná x je

- vázaná ve formuli $\varphi \equiv$ má vázaný výskyt ve φ.
- volná ve formuli $\varphi \equiv$ má volný výskyt ve φ.

Úmluva. Zápis $\varphi(x_1, \dots x_n)$ značí, že $x_1, \dots x_n$ jsou proměnné, jejichž volné výskyty nás ve formuli φ zajímají. Neznamená to, že každá z proměnných x_i musí mít volný výskyt ve φ, ani že φ neobsahuje žádné jiné volné proměnné.

Příklad. $\varphi = (\forall x)(\exists y)(x \leq y) \vee (x \leq z)$. Kvantifikátory se vztahují pouze k první závorce $(x \leq y)$. Proměnná x je vázaná a volná zároveň, y je vázaná a z je volná. Můžeme tedy psát $\varphi(x, z)$.

3 Axiomy Zermelo-Fraenkelovy teorie množin

Až doposud mohly množiny obsahovat libovolné „věci“ a vlastně jsme nijak nespecifikovali, co přesně jsou tyto věci zač. V axiomatické teorii množin existují pouze ty objekty, jejichž existence vyplývá z axiomů dané teorii. Axiomy ZF nám garantují existenci prázdné množiny a poskytují nám několik způsobů jak z již existujících množin vyrábět nové. Jinými slovy – všechno je množina. Každý prvek každé množiny je jen nějaká jiná množina.

3.1 Axiom existence

Axiom 1. *Existuje nějaká množina, univerzum množin není prázdné.*

$$(\exists x)(x = x).$$

3.2 Axiom extenzionality

Axiom 2. *Množina není dána ničím jiným než svými prvky.*

$$(\forall z)(z \in x \Leftrightarrow z \in y) \implies x = y.$$

Je důležité zdůraznit, že toto *není* definice identity dvou množin. Musíme vnímat odděleně dva koncepty. První koncept je naše teorie, ve které můžeme dokazovat různá pravdivá tvrzení. Je to něco zcela abstraktního. Druhý koncept je nějaká konkrétní „implementace“ (model) této teorie. Symbol '$=$' hovoří o identitě objektů, které poskytne ta konkrétní implementace. My „zevnitř“ naší teorie vůbec netušíme, jak by tato implementace mohla vypadat. Ale máme „zvenčí“ poskytnutý symbol $=$, který smíme používat. Každá implementaci „ví“, co tento symbol znamená. Ale neví, co znamená symbol $\in$. Axiomy jsou nějaké požadavky, které musí každý model splňovat. Takže tento axiom není definice identity dvou množin, protože identita je koncept, který je odtržený od teorie a přísluší až konkrétnímu modelu. Tento axiom vyjadřuje vztah symbolu $\in$ a identity a každý model bude muset tento požadavek splnit. Opačná implikace,

$$x = y \implies (\forall z)(z \in x \Leftrightarrow z \in y),$$

platí také, ale není součástí axiomu extenzionality, protože vlastně říká, že

$$(\forall z)(z \in x \Leftrightarrow z \in x),$$

což platí pro libovolnou implementaci symbolu $\in$.

3.3 Axiom dvojice

Axiom 3. *Pro každou dvojici množin x a y existuje množina d, která obsahuje právě x a y. Množinu d značíme jako $\{x, y\}$.*

$$(\forall x, y)(\exists d) : (\forall z)\big(z \in d \Leftrightarrow (z = x \vee z = y)\big).$$

Tento axiom zaručuje i existenci jednoprvkových množin $\{x\} \coloneqq \{x, x\}$.

3.4 Axiom sumy

Axiom 4. *Pro každou množinu x existuje množina s, která je sjednocením všech množin uvnitř x. Této množině říkáme suma množina x a značíme ji $\bigcup x$.*

$$(\forall x)(\exists s) : (\forall z)\big(z \in s \Leftrightarrow (\exists y)(y \in x \wedge z \in y)\big).$$

Pozorování. *Pokud $x \in y \in z$, potom $x \in \bigcup z$.*

Nyní můžeme pomocí kombinace axiomu sumy a axiomu dvojice definovat sjednocení dvou množin a libovolně velkou konečnou množinu danou výčtem.

Definice 5. Sjednocení množin x a y definujeme jako $x \cup y \coloneqq \bigcup\{x, y\}$.

Definice 6. Množiny $\{x_1\}$ a $\{x_1, x_2\}$ jsou garantované axiomem dvojice. Množinu $\{x_1, x_2, \dots x_n\}$ definujeme induktivně jako $\{x_1, x_2, \dots x_{n-1}\} \cup \{x_n\}$.

Příklad. $\bigcup\big\{\{x_1\}, \{x_1, x_2\}, \{x_2, x_3\}\big\} = \{x_1, x_2, x_3\}$.

3.5 Schéma axiomů vydělení

Schéma znamená, že se nejedná o jeden konkrétní axiom, ale o nekonečně mnoho různých axiomů, které mají všechny stejnou strukturu.

Axiom 5. *Pokud je x množina, potom existuje množina všech jejích prvků, které splňují formuli φ. Tuto množinu značíme $\{z \in x \mid \varphi(z)\}$. Formálně, je-li $\varphi(z)$ formule, která neobsahuje volně proměnnou y, potom formule*

$$(\forall x)(\exists y) : (\forall z)\big(z \in y \Leftrightarrow (z \in x \wedge \varphi(z))\big).$$

je axiom.

Všimněme si, že schéma axiomů vydělení nám nedovoluje vyrobit množinu všech množin nebo množinu všech krotkých množin, protože neumožňuje konstrukce typu $\{z \mid \varphi(z)\}$. Použitím axiomu vždy vznikne podmnožina nějaké již existující množiny. Například z množiny X, garantované axiomem existence, lze vyrobit prázdnou množinu tak, že za φ zvolíme libovolnou nesplnitelnou formuli.

Definice 7. Prázdná množina je $\varnothing \coloneqq \{z \in X \mid z \neq z\}$.

Také konečně můžeme nadefinovat průnik a rozdíl množin.

Definice 8. Rozdíl množin x a y je množina $x \setminus y \coloneqq \{z \in x \mid z \notin y\}$.

Definice 9. Průnik dvou množin x a y je množina $x \cap y \coloneqq \{z \in x \mid z \in y\}$.

Definice 10. Množiny x a y jsou disjunktní $\equiv x \cap y = \varnothing$.

Definice 11. Průnik množiny $x \neq \varnothing$ je množina $\bigcap x \coloneqq \bigl\{z \in \bigcup x \mid y \in x \Rightarrow z \in y\bigr\}$.

Příklad. Průnik konečně mnoha množin $x_1, x_2, \dots x_n$ lze zapsat dvěma způsoby:

$$\bigcap\{x_1, x_2, \dots x_n\} = x_1 \cap x_2 \cap \dots \cap x_n.$$

Průnik nekonečně mnoha množin už ovšem lze udělat pouze jako průnik nekonečné množiny x.

Poznámka. Důvod, proč zatím nedefinujeme průnik prázdné množiny je ten, že s touto definicí bychom měli $\bigcap \varnothing = \varnothing$, což moc nedává smysl. Prázdný součet je nula, prázdný součin je jedna a prázdná suma je prázdná množina. Vše to jsou neutrální prvky vůči dané operaci. Co je neutrální prvek vůči průniku? Prázdná množina určitě ne. Nabízí se množina všech množin, ale ukážeme, že ta neexistuje. Pokračování v sekci 4.2.

Definice 12. Uspořádaná dvojice (a, b) je množina $\{\{a\}, \{a, b\}\}$. Uspořádanou n-tici $(a_1, a_2, \dots a_n)$ potom definujeme induktivně jako $((a_1, a_2, \dots a_{n-1}), a_n)$.

Lemma 1. *Uspořádaná dvojice určuje svoje prvky jednoznačně. Tedy*

$$(x, y) = (a, b) \iff (x = a \wedge y = b).$$

Důkaz. Nejprve '$\Leftarrow$'. Z axiomu extenzionality máme $\{x\} = \{a\}$ a $\{x, y\} = \{a, b\}$ a tedy i $\{\{x\}, \{x, y\}\} = \{\{a\}, \{a, b\}\}$. Nyní '$\Rightarrow$'. Ukážeme, že (a,b) jednoznačně určuje pořadí svých prvků. Označme $P \coloneqq \bigcap(a,b)$ a $S \coloneqq \bigcup(a,b)$. Potom platí

$$\{a\} = P, \quad \{b\} = \{z \in S \mid z \neq a \vee P = S\}.$$

❑

3.6 Axiom potence

Axiom 6. *Pro každou množinu x existuje množina všech jejích podmnožin. Této množině říkáme potenční množina množiny x a značíme ji $\mathcal{P}(x)$.*

$$(\forall x)(\exists p) : (\forall z)(z \in p \Leftrightarrow z \subseteq x).$$

Pozorování. *Potenční množina a suma jsou svým způsobem opačné operace:*

$$z \subseteq x \Rightarrow z \in \mathcal{P}(x), \qquad z \in x \Rightarrow z \subseteq \bigcup x, \qquad \bigcup \mathcal{P}(x) = x \subseteq \mathcal{P}\bigl(\bigcup x\bigr)$$

3.7 Schéma axiomů nahrazení

Axiom 7. *Když si vezmu libovolné zobrazení f a množinu vzorů A, tak množina obrazů $B = f[A]$ je také množina. Formálně, je-li $\psi(x,y)$ formule, která neobsahuje volně proměnné y_1, y_2 a b, potom formule*

$$(\forall x)(\forall y_1,y_2)\bigl((\psi(x,y_1) \wedge \psi(x,y_2)) \Rightarrow y_1 = y_2\bigr) \Rightarrow \\ (\forall a)(\exists b) : (\forall y)\bigl(y \in b \Leftrightarrow (\exists x)(x \in a \wedge \psi(x,y))\bigr)$$

je axiom. Formule $\psi(x,y_1)$, resp. $\psi(x,y_2)$ vzniknou z formule $\psi(x,y)$ substitucí proměnné y_1, resp. y_2 za y.

První část tohoto axiomu říká, že $\psi(x,y)$ se má chovat jako zobrazení $y = f(x)$. Ve druhé polovině značí a množinu vzorů a b množinu obrazů, které těmto vzorům odpovídají.

Pozorování. *Pokud za $\psi(x,y)$ zvolíme formuli $x = y \wedge \varphi(y)$, tak je první část axiomu nahrazení splněna. Tedy platí, že*

$$(\forall a)(\exists b) : (\forall y)\big(y \in b \Leftrightarrow (\exists x)(x \in a \wedge x = y \wedge \varphi(y))\big),$$

což je jen trochu jinak zapsaný axiom vydělení.

3.8 Axiom fundovanosti

Axiom 8. *Každá neprázdná množina obsahuje nějakou množinu, která je s ní disjunktní.*

$$(\forall x \neq \varnothing)(\exists y \in x) : (x \cap y = \varnothing).$$

Důsledek. *Neexistuje množina a splňující $a \in a$.*

Důkaz. Pro spor nechť a je divoká. Potom množina $\{a\}$ nesplňuje fundovanost, protože $a \in a$ a zároveň $a \in \{a\}$, takže $a \in a \cap \{a\}$. ❏

Důsledek. *Neexistuje dvojice množin a, b taková, že $a \in b$ a $b \in a$. Tentokrát poruší fundovanost množina $\{a, b\}$.*

Tento axiom nám zaručuje, že v ZF nemůže vzniknout Russelův paradox, protože vylučuje možnost existence divokých a dalších divných množin. Také z něj vyplývá, že v ZF neexistuje množina všech množin, protože ta by určitě byla divoká.

3.9 Axiom nekonečna

Axiom 9. *Existuje nekonečná množina s nějakou konkrétní strukturou.*

$$(\exists w) : \big(\varnothing \in w \wedge (\forall z)(z \in w \Rightarrow z \cup \{z\} \in w)\big).$$

Axiom nekonečna nám umožní definovat množinu všech přirozených čísel, jako nejmenší množinu splňující tuto podmínku.

3.10 Axiom výběru a ZFC

Axiom výběru, anglicky Axiom of choice (AoC), je natolik silné tvrzení, že není součástí základní verze Zermelo-Fraenkelovy teorie. Jeho přidáním do ZF získáme mnohem silnější teorii ZFC. Bez něj nelze dokázat mnoho věcí, které by intuitivně měly platit, ale některé jeho důsledky jsou na hranici paradoxnosti, proto byl historicky velmi kontroverzní. Budeme se jím zabývat ve zvláštní kapitole.

4 Množiny vs. třídy

Dokázali jsme, že v ZF množina všech množin neexistuje. Ale chtěli bychom aby existovalo něco podobného, protože občas chceme mluvit o souboru všech objektů, které něco splňují, přestože to už není množina. Proto se zavádí pojem *třída*. V Cantorově naivní teorii jsou třídy a množiny jedno a totéž. Pokud omezíme co všechno může být množinou, tak se náš svět rozdělí.

- Množiny – někam náleží.
- Třídy – něco náleží do nich.

Uvědomme si, že tento koncept neumožňuje zrekonstruovat Russellův paradox, jelikož třída všech krotkých tříd zjevně neexistuje. Třídy totiž nemohou nikam náležet, věci pouze náleží do nich.

4.1 Rozšíření jazyka o třídové termy

Třída je pouze matajazykový pojem, v ZF nejsou formálně definované.

Definice 13 (Třída)**.** Pokud je $\varphi(x)$ formule, tak výraz $\{x \mid \varphi(x)\}$ nazýváme třídový term. Definuje „soubor" všech množin x, pro které platí $\varphi(x)$. Tomuto souboru říkáme třída určená formulí $\varphi(x)$.

Pozorování. *Pokud je $\varphi(x)$ ve tvaru $x \in y \wedge \psi(x)$, kde y je množina, tak třída $\{x \mid \varphi(x)\}$ je množina (z axiomu vydělení).*

Pozorování. *Každá množina je zároveň i třídou, protože $x = \{z \mid z \in x\}$.*

Definice 14. Třídu, která není množinou nazýváme vlastní třída.

Ve formulích na místě volných proměnný připustíme třídové termy. Navíc dovolíme třídové proměnné, které budeme značit velkými písmeny. Ale pouze jako volné proměnné, takže třídy není možné kvantifikovat.

Definice 15 (Formule s třídovými termy)**.** Atomické formule v tomto rozšířeném jazyce jsou

$$x = y, \quad x \in y, \quad x = X, \quad x \in X, \quad X \in x, \quad X = Y, \quad X \in Y,$$

kde x, y jsou proměnné, X je zkratka za $\{z \mid \varphi(z)\}$ a Y za $\{z \mid \psi(z)\}$.

Každá atomická formule je formule a libovolná kombinace formulí pomocí logických spojek je opět formule. Množinové proměnné lze navíc kvantifikovat.

Tvrzení 2. *Pro každou formuli s třídovými termy, ale bez třídových proměnných existuje ekvivalentní formule v základním jazyce.*

Důkaz. Eliminujeme třídové termy. Mějme množiny x, y, z, logické formule $\varphi(x)$ a $\psi(y)$ a třídové termy $X = \{x \mid \varphi(x)\}$ a $Y = \{y \mid \psi(y)\}$. Přepíšeme všechny atomické formule do základního jazyka.

- $z \in X \sim z \in \{x \mid \varphi(x)\} \sim \varphi(z)$,

- $X = Y \sim \{x \mid \varphi(x)\} = \{y \mid \psi(y)\} \sim (\forall u)(\varphi(u) \Leftrightarrow \psi(u))$.

Dále budeme využívat, že X nemůže být vlastní třída.

- $z = X \sim z = \{x \mid \varphi(x)\} \sim (\forall u)(u \in z \Leftrightarrow \varphi(u))$,
- $X \in Y \sim \{x \mid \varphi(x)\} \in \{y \mid \psi(y)\} \sim (\exists u)\big(u = \{x \mid \varphi(x)\} \wedge u \in \{y \mid \psi(y)\}\big) \sim (\exists u)\big((\forall v)(v \in u \Leftrightarrow \varphi(v)) \wedge \psi(u)\big)$,
- $X \in y \sim \{x \mid \varphi(x)\} \in y \sim (\exists u)\big(u = \{x \mid \varphi(x)\} \wedge u \in y\big) \sim (\exists u)\big((\forall v)(v \in u \Leftrightarrow \varphi(v)) \wedge u \in y\big)$.

❑

Důsledek. *Formule rozšířeného jazyka určují stejné třídy jako formule základního jazyka. Třídové termy slouží pouze pro usnadnění zápisu.*

Formule s třídovými proměnnými lze interpretovat jako schémata formulí základního jazyka. Za třídovou proměnnou totiž můžeme dokazit jakýkoli třídový term, který odpovídá nějaké formuli základního jazyka.

4.2 Třídové operace

Definice 16. Pro třídy A a B definujeme

- $A \cap B \coloneqq \{x \mid x \in A \wedge x \in B\}$,
- $A \cup B \coloneqq \{x \mid x \in A \vee x \in B\}$,
- $A \setminus B \coloneqq \{x \mid x \in A \wedge x \notin B\}$, …případně $A - B$
- $\bigcup A \coloneqq \{x \mid (\exists a)(a \in A \wedge x \in a)\}$,
- $\bigcap A \coloneqq \{x \mid (\forall a)(a \in A \Rightarrow x \in a)\}$
- $A \subseteq B \equiv (\forall x)(x \in A \Rightarrow x \in B)$, …$A$ je podtřídou B
- $A \subset B \equiv A \subseteq B \wedge A \neq B$, …$A$ je vlastní podtřídou B
- $\mathcal{P}(A) \coloneqq \{x \mid x \subseteq A\}$.

Pozorování. *Průnik prázdné množiny je třída všech množin.*

Definice 17 (Univerzální třída)**.** Třídu všech množin $V \coloneqq \{x \mid x = x\}$ nazýváme univerzální třída. Třídu $V \setminus A$ nazýváme absolutní doplněk třídy A.

Pozorování. *Platí $\mathcal{P}(V) = V$.*

Důkaz. Nechť x je libovolná množina. Ukážeme, že $x \in \mathcal{P}(V)$. Platí to, protože $(\forall z)(z \in x \Rightarrow z \in V)$, tedy $x \subseteq V$, z čehož $x \in \mathcal{P}(V)$.

❑

Lemma 3. *Je-li a množina a $A = \{x \mid \varphi(x)\}$ třída, potom je $a \cap A$ množina.*

Důkaz. Z axiomu vydělení máme $a \cap A = \{x \in a \mid \varphi(x)\}$.

❑

4.3 Kartézský součin

Definice 18. Kartézský součin tříd A a B je třída

$$A \times B \coloneqq \{(a,b) \mid a \in A \wedge b \in B\}.$$

Kartézský součin tříd $A_1, A_2, \dots A_n$ definujeme induktivně jako

$$A_1 \times \dots \times A_n \coloneqq (A_1 \times \dots \times A_{n-1}) \times A_n = \{(a_1, \dots a_n) \mid \textstyle\bigwedge_{i=1}^n a_i \in A_i\}.$$

Lemma 4. *Jsou-li x a y množiny, potom je $x \times y$ také množina.*

Důkaz. Idea těchto důkazů: najít nějakou hodně velkou množinu a pak použít axiom vydělení. Dokážeme, že platí

$$x \times y \subseteq \mathcal{P}(\mathcal{P}(x \cup y)).$$

Uspořádanou dvojici jsme definovali jako $(a,b) = \{\{a\},\{a,b\}\}$. Pokud $a \in x$ a $b \in y$, tak $\{a\},\{a,b\} \subseteq x \cup y$ neboli $\{a\},\{a,b\} \in \mathcal{P}(x \cup y)$. Tedy $(a,b) \subseteq \mathcal{P}(x \cup y)$, z čehož $(a,b) \in \mathcal{P}(\mathcal{P}(x \cup y))$.

❑

Definice 19 (Kartézská mocnina)**.** Pro třídu X definujeme $X^1 \coloneqq X$ a pak induktivně $X^n \coloneqq X^{n-1} \times X = \prod_{i=1}^n X$.

Pozorování. *Pro univerzální třídu platí $V = V^1 \supseteq V^2 \supseteq V^3 \supseteq \cdots$.*

Důkaz. Každá n-tice je i dvojice (tak je definovaná), ale lze ji dokonce vnímat jako k-tici pro libovolné $k \leq n$. Například jako trojici $(a,b,c) = ((a,b),c)$:

$$(x_1, \dots x_{n-1}, x_n) = ((x_1, \dots x_{n-1}), x_n) = (((x_1, \dots x_{n-2}), x_{n-1}), x_n).$$

❑

Příklad. Definujeme $X^3 \coloneqq X^2 \times X$, ale $X \times X^2 \neq X^3$. Mají stejnou strukturu, ale v teorii množin to jsou různé objekty. Zvolme třeba $X = \{\emptyset\}$. Máme

- $X^2 \times X = \{(\emptyset,\emptyset)\} \times \{\emptyset\} = \{((\emptyset,\emptyset),\emptyset)\}$,
- $X \times X^2 = \{\emptyset\} \times \{(\emptyset,\emptyset)\} = \{(\emptyset,(\emptyset,\emptyset))\}$.

4.4 Relace a zobrazení

Definice 20. Rozšíříme náš jazyk o další zkratky. Nechť A je třída a φ formule.

- $(\exists x \in A)(\varphi) \equiv (\exists x)(x \in A \wedge \varphi)$,
- $(\nexists x \in A)(\varphi) \equiv (\forall x)(x \notin A \vee \neg\varphi)$,
- $(\forall x \in A)(\varphi) \equiv (\forall x)(x \in A \Rightarrow \varphi)$.

Poslední zkratku definujeme pouze pro formule $\varphi(x)$ bez volných výskytů y a z:

- $(\exists! x \in A)(\varphi) \equiv (\exists x \in A)(\varphi) \wedge (\forall y \in A)(\forall z \in A)\big((\varphi(y) \wedge \varphi(z)) \Rightarrow y = z\big)$.

Definice 21. Binární relace je libovolná třída $R \subseteq V \times V$. Namísto $(x,y) \in R$ píšeme $x\,R\,y$. Podobně lze definovat n-ární relaci jako $R \subseteq V^n$.

Definice 22. Pro (binární) relaci R a třídu X definujeme třídy

- $R^{-1} \coloneqq \{(v,u) \mid u\,R\,v\}$, ... inverzní relace k relaci R
- $\mathrm{Dom}(R) \coloneqq \{u \mid (\exists v)(u\,R\,v)\}$, ... definiční obor relace R
- $\mathrm{Rng}(R) \coloneqq \{v \mid (\exists u)(u\,R\,v)\}$, ... obor hodnot relace R
- $R \restriction X \coloneqq R \cap (X \times V) \subseteq R$, ... zúžení relace R na třídu X
- $R[X] \coloneqq \mathrm{Rng}(R \restriction X) \subseteq \mathrm{Rng}(R)$. ... obraz třídy X relací R

Pozorování. $R \subseteq \mathrm{Dom}(R) \times \mathrm{Rng}(R), \quad R^{-1} \subseteq \mathrm{Rng}(R) \times \mathrm{Dom}(R)$.

Lemma 5. *Pokud je relace x množina a Y třída, potom x^{-1}, $\mathrm{Dom}(x)$, $\mathrm{Rng}(x)$, ale i $x \restriction Y$ a $x[Y]$ jsou také množiny.*

Důkaz. Pomocí axiomu vydělení.

- Ukážeme $\mathrm{Dom}(x) \subseteq \bigcup(\bigcup x)$. Pro libovolné $u \in \mathrm{Dom}(x)$ existuje v t.ž. $(u,v) \in x$. Máme posloupnost inkluzí $u \in \{u\} \in (u,v) \in x$, tedy $u \in \bigcup(\bigcup x)$.
- Podobně $\mathrm{Rng}(x) \subseteq \bigcup(\bigcup x)$, zkrátka to $v \in \mathrm{Rng}(x)$ je třeba vybalit z té uspořádané dvojice $(u,v) \in x$ jako $v \in \{u,v\} \in (u,v) \in x$.
- $x^{-1} \subseteq \mathrm{Rng}(x) \times \mathrm{Dom}(x)$ ... kartézský součin množin je množina.
- $x[Y] \subseteq \mathrm{Rng}(x)$ a $x \restriction Y \subseteq x$. ❏

Definice 23. Relace odpovídající relačním symbolům jazyka teorie množin jsou

- $\mathrm{E} \coloneqq \{(x,y) \mid x \in y\}$, ... náležení
- $\mathrm{Id} \coloneqq \{(x,y) \mid x = y\}$. ... identita
- $\Delta_X \coloneqq \mathrm{Id} \restriction X$ ... identita na třídě X

Definice 24 (Skládání relací)**.** Pro relace R a S definujeme relaci

$$R \circ S \coloneqq \{(u,w) \mid (\exists v)(u\,R\,v \wedge v\,S\,w)\}$$

Příklad. $\mathrm{Id} \circ R = R \circ \mathrm{Id} = R, \quad (x,y) \in \mathrm{E} \circ \mathrm{E} \iff x \in \bigcup y$.

Definice 25 (Zobrazení)**.** Relace F je zobrazení (funkce) $\equiv$

$$(\forall u)(\forall v)(\forall w)\big(((u,v) \in F \wedge (u,w) \in F) \Rightarrow v = w\big).$$

Namísto $u\,F\,v$ píšeme $F(u) = v$, při definování píšeme $F : u \mapsto v$.

Pozorování. *F je zobrazení* $\iff (\forall x \in \mathrm{Dom}(F))(\exists! y \in \mathrm{Rng}(F))(F(x) = y)$.

Definice 26 (Prosté zobrazení, bijekce)**.** Řekneme, že zobrazení F je

- prosté $\equiv F^{-1}$ je zobrazení, ...injekce
- zobrazení třídy X do třídy $Y \equiv \mathrm{Dom}(F) = X \wedge \mathrm{Rng}(F) \subseteq Y$, píšeme $F : X \to Y$,
- zobrazení třídy X na třídu $Y \equiv F : X \to Y \wedge \mathrm{Rng}(F) = Y$, ...surjekce
- bijekce mezi třídami X a $Y \equiv$ je to prosté zobrazení X na Y.

Pozorování. *Pokud je F prosté, potom je F^{-1} také prosté.*

Lemma 6. *Pokud je f zobrazení a* $\mathrm{Dom}(f)$ *množina, potom f je také množina.*

Důkaz. Axiom nahrazení nám říká, že zobrazení zobrazují množiny na množiny, tedy $f[\mathrm{Dom}(f)] = \mathrm{Rng}(f)$ je množina a z axiomu vydělení je tedy $f \subseteq \mathrm{Dom}(f) \times \mathrm{Rng}(f)$ také množina. ❑

Definice 27 (Třída zobrazení mezi množinami)**.** Pro třídu A a množinu a definujeme třídu všech zobrazení z množiny a do třídy A jako

$$^{a}A := \{f \mid f : a \to A\}.$$

Poznámka. Nelze definovat ^{B}A pokud B je vlastní třída, potom by ta zobrazení $f : B \to A$ už byla vlastní třídy. Obměnou f množina $\Rightarrow \mathrm{Dom}(f)$ množina.

Pozorování. *Pokud jsou A a B konečné množiny, tak je $\left|^{B}A\right| = |A|^{|B|}$.*

Příklad. $^{\varnothing}A = \{\varnothing\}$ a $^{a}\varnothing = \varnothing$, ovšem $^{\varnothing}\varnothing = \{\varnothing\}$. ...$0^0 := 1$.

Lemma 7. *O velikosti třídy zobrazení.*

1. *Pro libovolné množiny x, y je ^{x}y množina.*
2. *Je-li $x \neq \varnothing$ a Y vlastní třída, potom je ^{x}Y vlastní třída.*

Důkaz. První část pomocí axiomu vydělení, druhá pomocí nahrazení.

1. $f : x \to y$, pak $f \subseteq x \times y$, tedy $f \in \mathcal{P}(x \times y)$, takže $^{x}y \subseteq \mathcal{P}(x \times y)$. Využíváme, že kartézský součin množin je množina.
2. Pro každé $y \in Y$ definujeme konstantní zobrazení $K_y : x \to Y$ jako $u \mapsto y$, neboli $K_y = x \times \{y\}$. Protože $x \neq \varnothing$, tak pro $y_1 \neq y_2$ je $K_{y_1} \neq K_{y_2}$. Označme $K := \{K_y \mid y \in Y\}$. Zřejmě $K \subseteq {}^{x}Y$. Sporem ukážeme, že K je vlastní třída, (takže ^{x}Y taky). Předpokládejme, že K je množina a definujme zobrazení $F : K \to Y, K_y \mapsto y$. Protože předpokládáme, že K je množina, tak z axiomu nahrazení je i Y množina, ale to je spor. ❑

Definice 28 (Vlastnosti relací)**.** Nechť $R \subseteq V \times V$ je relace a X třída. Označme $R_X := R \restriction X$. Řekneme, že relace R je na X

- reflexivní $\equiv \Delta_X \subseteq R$,

- antireflexivní $\equiv \Delta_X \cap R = \varnothing$,
- symetrická $\equiv R_X = R_X^{-1}$,
- slabě antisymetrická $\equiv R_X \cap R_X^{-1} \subseteq \Delta_X$,
- silně antisymetrická $\equiv R_X \cap R_X^{-1} = \varnothing$,
- tranzitivní $\equiv R_X \circ R_X \subseteq R_X$.

Pozorování. *Tyto vlastnosti jsou dědičné, neboli platí na každé podtřídě $Y \subseteq X$.*

4.5 Uspořádání

Definice 29 (Uspořádání)**.** Relace $R \subseteq V \times V$ je na třídě X

- trichotomická $\equiv (\forall x,y \in X)(x \, R \, y \vee y \, R \, x \vee x = y)$,
- ostré uspořádání $\equiv$ je antireflexivní a tranzitivní na X,
- uspořádání $\equiv$ je reflexivní, slabě antisymetrická a tranzitivní na X,
- lineární uspořádání $\equiv$ je trichotomická a uspořádání na X.

Pokud je R uspořádání, tak místo $x \, R \, y$ píšeme $x \leq_R y$. Dále definujme ostré uspořádání $R' := R \setminus \mathrm{Id}$. Namísto $x \, R' \, y$ píšeme $x <_R y$.

Pozorování. *Každé ostré uspořádání R je silně antisymetrické.*

Důkaz. Kdyby ne, tak existují $x, y \in X$ t.ž. $x \, R \, y$ a $y \, R \, x$. Z tranzitivity $x \, R \, x$, což je spor s antireflexibilitou. ❑

Úmluva. Všimněme si, že pokud je R ostré uspořádání, potom není uspořádání. Pokud nějakému ostrému uspořádání budeme přiřazovat vlastnosti uspořádání, například budeme hovořit o dobrém ostrém uspořádání R, tak tím myslíme, že $R \cup \mathrm{Id}$ je dobré uspořádání.

Příklad. Identita není ostré uspořádání, protože není antireflexivní. Identita je uspořádání. Ale ne lineární, protože různé prvky nejsou porovnatelné. Náležení není uspořádání (ani ostré uspořádání), protože není tranzitivní.

Definice 30. Nechť R je uspořádání na třídě A a $X \subseteq A$. Prvek $a \in A$ je

- horní mez třídy $X \equiv (\forall x \in X)(x \leq_R a)$, ...také majoranta
- maximální prvek třídy $X \equiv a \in X \wedge (\nexists x \in X)(a <_R x)$,
- největší prvek třídy $X \equiv a \in X$ a je to horní mez X,
- supremum třídy $X \equiv$ je nejmenší prvek třídy všech horní mezí X.

Největší prvek, resp. supremum značíme $\max_R(X)$, resp. $\sup_R(X)$; pokud existují. Obdobně definujeme minorantu, minimální prvek, nejmenší prvek a infimum.

Pozorování. *Každý největší prvek je maximální. Pokud je R lineární uspořádání, tak maximální prvek je nejvýše jeden a pokud existuje, tak je největší. Největší prvek i supremum je vždy nejvýše jedno.*

Definice 31 (Dolní množina)**.** Nechť R je uspořádání na třídě A. Třída $X \subseteq A$ je

- shora omezená v $A \equiv$ existuje $a \in A$ horní mez X,
- dolní množina v $A \equiv (\forall x \in X)(\forall a \in A)(a \leq_R x \Rightarrow a \in X)$.

Každý prvek $a \in A$ určuje dolní množinu

$$(\leftarrow, a] \coloneqq \{x \mid x \in A \wedge x \leq_R a\}.$$

Pozorování. *Sjednocení dolních množin je dolní množina.*

Pozorování. *Nechť R je uspořádání na třídě A. Pak pro libovolné $x, y \in A$ platí*

$$x \leq_R y \iff (\leftarrow, x] \subseteq (\leftarrow, y].$$

Čili uspořádání $\subseteq$ na $\mathcal{P}(A)$ je svým způsobem univerzální. Každé uspořádání lze převést na inkluzi.

Definice 32. Řekneme, že uspořádání R je na množině A

- husté $\equiv (\forall x, y \in A)\big(x < y \Rightarrow (\exists z \in A)(x < z < y)\big)$,
- dobré $\equiv$ každá neprázdná $B \subseteq A$ má nejmenší prvek,
- úplné $\equiv$ každá neprázdná, shora omezená $B \subseteq A$ má supremum.

Pokud je $\leq$ lineární, resp. dobré uspořádání množiny A, tak říkáme, že $(A, \leq)$ je lineárně, resp. dobře uspořádaná množina. Pokud existuje nějaké úplné uspořádání množiny A, tak říkáme, že A je úplná.

Pozorování. *Všechny tyto vlastnosti jsou dědičné.*

Pozorování. *Každé dobré uspořádání je lineární. Kdyby nebylo, tak by existovaly nějaké dva neporovnatelné prvky a množina těchto dvou prvků by neměla nejmenší prvek.*

4.6 Vlastnosti známých uspořádání

Níže je uvedeno několik známých uspořádání a jejich vlastnosti.

- $(\mathbb{N}, \leq)$ Přirozená čísla se standardní interpretací $\leq$ je dobře uspořádaná množina. Její nejmenší prvek je nula.
- $(\mathbb{Z}, \leq)$ Standardní uspořádání celých čísel je lineární, ale není dobré, protože vůči $\leq$ neexistuje nejmenší celé číslo.
- $(\mathbb{Z}, \preceq)$ Uspořádání $x \preceq y \equiv (|x| < |y|) \vee (|x| = |y| \wedge x \leq y)$ celých čísel je dobré. Toto uspořádání vypadá následovně: $0, -1, 1, -2, 2, -3, 3, \ldots$

- $(\mathbb{Q}, \ \leq)$ Standardní uspořádání racionálních čísel je lineární a husté, ale není dobré, protože $\mathbb{Q}$ nemá žádný nejmenší prvek vůči $\leq$. Ovšem není těžké sestrojit nějaké dobré uspořádání. Racionální čísla nejsou úplná.
- $(\mathbb{R}, \ \leq)$ Standardní uspořádání reálných čísel je lineární, husté a úplné. Ale není dobré a dokonce ani nevíme, jestli v ZF nějaké dobré uspořádání reálných čísel vůbec existuje.
- $(\mathbb{N}^+, |\,)$ Přirozená čísla bez nuly spolu s relací dělitelnosti jsou částečné uspořádání. Toto uspořádání nemá žádný maximální prvek, ale zato má nejmenší prvek, a sice jedničku.
- $(\mathcal{P}(A), \subseteq)$ Potenční množina libovolné množiny A spolu s inkluzí je částečně uspořádaná množina. V tomto uspořádání je prázdná množina $\varnothing$ nejmenší prvek a A největší prvek.
- $(\Sigma^*, \ \leq_{LEX})$ Lexikografické uspořádání konečných řetězců nad abecedou Σ je dobré uspořádání. Nejmenší prvek je prázdný řetězec.

4.7 Dedekindovy řezy

Níže předvedeme jednu z možných konstrukcí $\mathbb{R}$ z $\mathbb{Q}$, konkrétně pomocí Dedekindových řezů. Předpokládejme, že $\mathbb{Q}$ už máme.

Definice 33. Množina $X \subseteq \mathbb{Q}$ je Dedekindův řez $\equiv$

1. X je dolní množina $\mathbb{Q}$,
2. existuje-li $\sup_{\mathbb{Q}}(X)$, potom $\sup_{\mathbb{Q}}(X) \in X$.

Takže třeba $\mathbb{Q} \cap (-\infty, 1)$ není dd. řez, ale $\mathbb{Q} \cap (-\infty, 1]$ ano. Jinak by to nebylo jednoznačné. Ovšem $\mathbb{Q} \cap (-\infty, \sqrt{2}) = \mathbb{Q} \cap (-\infty, \sqrt{2}]$ je dd. řez, protože tato množina nemá v $\mathbb{Q}$ supremum.

Definice 34. Reálná čísla definujeme jako $\mathbb{R} \coloneqq \{x \in \mathcal{P}(\mathbb{Q}) \,|\, \text{x je Dedekindův řez}\}$.

My s reálnými čísly ovšem většinou budeme pracovat spíše jako s nekonečnými binárními zápisy.

4.8 Ekvivalence a kvaziuspořádání

Definice 35. Relace $R \subseteq V \times V$ je na třídě X

- kvaziuspořádání $\equiv$ je reflexivní a tranzitivní na X,
- ekvivalence $\equiv$ je reflexivní, symetrická a tranzitivní na X.

Definice 36 (Třídy ekvivalence)**.** Nechť R je ekvivalence na třídě X. Pro $x \in X$ definujeme třídu

$$[x]_R \coloneqq \{y \,|\, y \in X \wedge x\,R\,y\} = R[\{x\}] \cap X,$$

kterou nazýváme ekvivalenční třída prvku x. Pokud je X množina, tak z axiomu vydělení je $[x]_R$ také množina. V tom případě definujeme množinu ekvivalenčních tříd množiny X podle ekvivalence R jako

$$X/R \coloneqq \{[x]_R \in \mathcal{P}(X) \,|\, x \in X\}.$$

Definice 37. Rozklad množiny X je libovolná množina $\mathcal{R} \subseteq \mathcal{P}(X)$ t.ž.

1. $(\forall a \in \mathcal{R})(a \neq \varnothing)$,
2. $(\forall a,b \in \mathcal{R})(a \neq b \Rightarrow a \cap b = \varnothing)$,
3. $\bigcup \mathcal{R} = X$.

Lemma 8. *Pokud je $\sim$ ekvivalence na množině X, potom je $X/\sim$ rozklad X.*

Důkaz. Musíme ukázat, že $X/\sim$ splňuje definici rozkladu.

1. Z reflexivity $x \sim x$, tedy $x \in [x]$ pro každé $[x] \in X/\sim$.
2. Obměnou: ukážeme $[x] \cap [y] \neq \varnothing \Rightarrow [x] = [y]$. Chceme ukázat, že pokud existuje $t \in [x] \cap [y]$ a $a \in [x]$, potom $a \in [y]$. Víme, že $a \sim x$, $x \sim t$, $t \sim y$ a tudíž z tranzitivity $a \sim y$. Použili jsme i symetrii.
3. Stačí ukázat, že pokud $x \in X$, potom existuje $a \in X/\sim$ t.ž. $x \in a$. Ale toto a je prostě $[x]$.

❑

Pozorování. *Pokud je relace $\lesssim$ kvaziuspořádání na množině X, potom můžeme definovat ekvivalenci $\sim$ na X předpisem*

$$x \sim y \equiv x \lesssim y \wedge y \lesssim x.$$

Potom můžeme definovat uspořádání $\leq$ na množině $X/\sim$ jako

$$[x]_\sim \leq [y]_\sim \equiv x \lesssim y.$$

Tato konstrukce je velmi šikovná, často se totiž potýkáme s množinou X, která je skoro uspořádaná relací R, až na to, že R není antisymetrická na některých podmnožinách X. Potom prostě prohlásíme tyto zlobivé prvky za ekvivalentní a definujeme nové uspořádání na třídách ekvivalence.

Ovšem pokud je X vlastní třída, tak to nemusí fungovat. Může se stát, že pro nějaké $x \in X$ bude $[x]_\sim$ také vlastní třída, a potom nelze definovat $X/\sim$.

5 Srovnávání mohutnosti množin

Definice 38. Pro množiny x a y definujeme relace

1. $x \approx y \equiv$ existuje bijekce $f : x \to y$,
2. $x \preceq y \equiv$ existuje prosté zobrazení $f : x \to y$,
3. $x \prec y \equiv x \preceq y \wedge x \not\approx y$.

Poznámka. Pro třídy tato definice nemá smysl, protože je nelze kvantifikovat.

Poznámka. Relaci $x \preceq y$ jsme také mohli definovat jako „existuje zobrazení y na x“. Ale potom by věta 11 nešla dokázat bez AoC. Důvod je následující.

Platí: Existuje-li prosté zobrazení x do y, potom existuje zobrazení y na x. Prostě vezmu ten jednoznačně určený prvek. Ale opačný směr bez AoC neplatí, protože se na jeden prvek může zobrazit až nekonečně mnoho prvků a tohle se může stát nekonečně-mnoho krát, takže to prosté zobrazení v opačném směru bez AoC nesestrojím.

Pozorování. *Pro libovolné množiny x, y, z platí*

- $x \subseteq y \implies x \preceq y$,
- $x \subset y \implies x \preceq y$, *. . . ale ne $x \prec y$*
- $x \approx x$, *. . . identitou*
- $x \approx y \implies y \approx x$, *. . . inverzní bijekcí*
- $(x \approx y \wedge y \approx z) \implies x \approx z$, *. . . složení bijekcí je bijekce*
- $x \preceq x$, *. . . identitou*
- $(x \preceq y \wedge y \preceq z) \implies x \preceq z$, *. . . složení prostých zobr. je prosté*
- $\preceq$ *je trichotomická* $\iff$ *platí axiom výběru.* *. . . což dokážeme*

Důsledek. *Relace $\approx$ je ekvivalence a $\preceq$ je kvaziuspořádání. Ale ne uspořádání, protipříklad na antisymetrii je třeba $\{\varnothing\}$ a $\{\{\varnothing\}\}$.*

Příklad. Mohli bychom z kvaziuspořádání $\preceq$ vyrobit uspořádání na ekvivalenčních třídách $[x]_\approx$? Bohužel ne, protože to jsou vlastní třídy, takže $V/\approx$ neexistuje. Kdyby pro nějaké $x \neq \varnothing$ byla $[x]_\approx$ množina, tak $V = \bigcup [x]_\approx$ by také byla množina.

Lemma 9. *Nechť x, y, x_1, y_1 a z jsou množiny. Pak*

1. $x \times y \approx y \times x$,
2. $x \times (y \times z) \approx (x \times y) \times z$,
3. $(x \approx x_1 \wedge y \approx y_1) \implies (x \times y) \approx (x_1 \times y_1)$,
4. $x \approx y \implies \mathcal{P}(x) \approx \mathcal{P}(y)$,
5. $\mathcal{P}(x) \approx {}^x 2$. *. . .* $2 = \{0, 1\} = \{\varnothing, \{\varnothing\}\}$

Důkaz. Vždy sestrojíme nějakou bijekci h.

1. $h : (u, v) \mapsto (v, u)$,
2. $h : (a, (b, c)) \mapsto ((a, b), c)$,
3. $f : x \to x_1$ a $g : y \to y_1$. Uděláme $h : (a, b) \mapsto (f(a), g(b))$,
4. $f : x \to y$. Uděláme $h : u \mapsto f[u]$,
5. Pro $u \subseteq x$ definujeme charakteristickou funkci $\chi_u : x \to \{0, 1\}$ předpisem

$$\chi_u(a) \coloneqq \begin{cases} 1, & a \in u, \\ 0, & a \notin u. \end{cases}$$

Bijekci $h : \mathcal{P}(x) \to {}^x2$ definujeme jako $h : u \mapsto \chi_u$. ❑

5.1 Cantor-Schröder-Bernsteinova věta

Definice 39 (Monotónní zobrazení)**.** Zobrazení $H : \mathcal{P}(x) \to \mathcal{P}(y)$ je monotónní vzhledem k inkluzi $\equiv$ pro všechny u,$v \subseteq x$ platí

$$u \subseteq v \Rightarrow H(u) \subseteq H(v).$$

Příklad. $A \subseteq \mathcal{P}(x)$ uspořádaná pomocí $\subseteq$, pak $\sup_{\subseteq}(A) = \bigcup A$ a $\inf_{\subseteq}(A) = \bigcap A$.

Lemma 10 (O pevném bodu)**.** *Je-li $H : \mathcal{P}(x) \to \mathcal{P}(x)$ monotónní vzhledem k inkluzi, pak existuje $c \in \mathcal{P}(x)$ t.ž. $H(c) = c$.*

Intuice. Představme si na chvíli, že H je funkce reálných čísel a chceme najít její pevný bod. Potom dává smysl se podívat na množinu $\{x \,|\, x \leq H(x)\}$. Nemělo by nás překvapit, kdyby supremum této množiny byl pevný bod.

Důkaz. Nechť $A \coloneqq \{u \in \mathcal{P}(x) \,|\, u \subseteq H(u)\}$ a označme $c \coloneqq \sup_{\subseteq}(A) = \bigcup A$. Ukážeme, že $H(c) = c$. Pro každou $u \in A$ platí

$$\begin{aligned} u &\subseteq c, && c \text{ je horní mez } A && (1)\\ u &\subseteq H(u), && u \in A \\ H(u) &\subseteq H(c), && H \text{ je monotónní} \\ u &\subseteq H(c). && \text{z předchozích dvou} \end{aligned}$$

Tedy $H(c)$ je horní mez A. Protože c je nejmenší horní mez A, tak platí

$$\begin{aligned} c &\subseteq H(c), && c \text{ je supremum } A \\ H(c) &\subseteq H(H(c)), && H \text{ je monotónní} && (2)\\ H(c) &\in A, && \text{podle 2} \\ H(c) &\subseteq c. && \text{podle 1} \end{aligned}$$

Máme inkluzi v obou směrech, takže $c = H(c)$. ❑

Věta 11 (Cantor, Schröder, Bernstein). $x \approx y \iff (x \preceq y \wedge y \preceq x)$.

Důkaz. Směr '$\Rightarrow$' je triviální. Pro '$\Leftarrow$' nechť $f : x \to y$ a $g : y \to x$ jsou prostá zobrazení. Uvažme „indukovaná“ zobrazení

$$\begin{aligned} \mathbf{f} : \mathcal{P}(x) &\to \mathcal{P}(y) \\ u &\mapsto f[u], \end{aligned} \qquad \begin{aligned} \mathbf{g} : \mathcal{P}(y) &\to \mathcal{P}(x) \\ v &\mapsto g[v]. \end{aligned}$$

Například $\mathbf{f}(\{1,2,3\}) = \{f(1), f(2), f(3)\}$. Všimněme si, že $\mathbf{f}$ i $\mathbf{g}$ jsou monotónní vzhledem k inkluzi. Chceme zobrazit kus x pomocí $\mathbf{f}$ na kus y a zbytek y zobrazit pomocí $\mathbf{g}$ zpátky na zbytek x. Ale obecně to nemusí dohromady vyplnit celou množinu x a můžou tam být nějaké duplicity.

Definujme zobrazení $H : \mathcal{P}(x) \to \mathcal{P}(x)$ jako $H : u \mapsto x - \mathbf{g}(y - \mathbf{f}(u))$. Dělá to, co je popsané výše a na konci vezme doplněk. Naším cílem je najít nějaké $c \subseteq x$, aby $H(c) = c$, tedy c a $\mathbf{g}(y - \mathbf{f}(c))$ tvoří rozklad x. Stačí ukázat, že H je monotónní vzhledem k inkluzi. Vezměme libovolné $u \subseteq v \subseteq x$. Máme

$$\begin{aligned} \mathbf{f}(u) &\subseteq \mathbf{f}(v), && \mathbf{f} \text{ je monotónní} \\ y - \mathbf{f}(u) &\supseteq y - \mathbf{f}(v), && \text{doplněk do } y \\ \mathbf{g}(y - \mathbf{f}(u)) &\supseteq \mathbf{g}(y - \mathbf{f}(v)), && \mathbf{g} \text{ je monotónní} \\ H(u) &\subseteq H(v). && \text{doplněk do } x \end{aligned}$$

Podle lemmatu 10 má H pevný bod, označme jej c. Tedy $c = x - \mathbf{g}(y - \mathbf{f}(c))$, takže $g[y - \mathbf{f}(c)] = x - c$. To znamená, že restrikce $g \restriction (y - \mathbf{f}(c))$ je prosté zobrazení $y - \mathbf{f}(c)$ na $x - c$, čili bijekce. Inverze bijekce je opět bijekce, tedy $g^{-1} \restriction (x - c)$ je bijekce mezi $x - c$ a $y - f[c]$. To doplníme bijekcí $f \restriction c$ mezi c a $f[c]$, čímž získáme bijekci $h \coloneqq (f \restriction c) \cup (g^{-1} \restriction (x - c))$ mezi x a y:

$$h(a) = \begin{cases} f(a), & a \in c, \\ g^{-1}(a), & a \in x - c. \end{cases}$$

❑

5.2 Příklady na srovnávání mohutností

Množinu přirozených čísel danou axiomem nekonečna budeme značit ω. Ovšem pokud budeme chtít o přirozených číslech mluvit jako o *číslech* a ne jako o *množinách*, tak budeme stále používat značení $\mathbb{N}$.

Příklad. $\omega \approx \omega \times \omega$. Využijeme větu 11 a definujeme prostá zobrazení

$$\begin{aligned} f : \omega &\to \omega \times \omega \\ n &\mapsto (n, 0), \end{aligned} \qquad \begin{aligned} g : \omega \times \omega &\to \omega \\ (a, b) &\mapsto 2^a \cdot 3^b. \end{aligned}$$

Zobrazení g je prosté ze základní věty aritmetiky.

Příklad. $\omega \approx \mathbb{Q}$. Zlomky jsou vlastně uspořádané trojice $\mathbb{Q} \subseteq \omega \times \omega \times 2$. Například $-3/4 \sim (3,4,1)$ nebo $4/8 \sim (4,8,0)$. Definujeme prostá zobrazení

$$\begin{aligned} f : \omega &\to \mathbb{Q} \\ n &\mapsto (n, 1, 0), \end{aligned} \qquad \begin{aligned} g : \mathbb{Q} &\to \omega \\ (a, b, s) &\mapsto 2^a \cdot 3^b \cdot 5^s. \end{aligned}$$

Čili $\omega \preceq \mathbb{Q}$ a zároveň $\mathbb{Q} \preceq \omega$, tedy podle Cantor-Bernsteinovy věty $\omega \approx \mathbb{Q}$.

Příklad. $[0,1]^2 \approx [0,1]$, tedy čtverec se zobrazí na úsečku. Hezké vysvětlení je ZDE.

Lemma 12. *Pokud pro množinu x platí $x \times x \approx x$, tak $x^n \approx x$ pro každé $n \in \mathbb{N}$.*

Důkaz. Když $n = 1$, tak hledaná bijekce je identita. Předpoklad nám dává bijekci $f_2 : x^2 \to x$, pomocí které induktivně definujeme bijekce $f_{n+1} : x^{n+1} \to x$ jako

$$f_{n+1} : (a_1, \dots a_{n+1}) \mapsto f_2(f_n(a_1, \dots a_n), a_{n+1}).$$

❑

5.3 Konečné množiny

5.3.1 Definice konečnosti

Nejpřirozenější definice je: x je konečná $\equiv (\exists n \in \omega)(x \approx n)$. My to uděláme trochu oklikou, protože s touto definicí se špatně dokazují věci.

Definice 40 (Tarski)**.** Množina x je konečná $\equiv$ každá neprázdná $a \subseteq \mathcal{P}(x)$ má maximální prvek vůči inkluzi. Pokud je x konečná, tak píšeme $\mathrm{Fin}(x)$.

Intuice. Tohle zjevně platí pro všechny konečné množiny. Vyberu nějaký prvek. Pokud je maximální, vyhrál jsem. Pokud není, tak existuje větší, vyberu jej a opakuji. Ale třeba pro množinu přirozených čísel $\mathbb{N}$ to už neplatí. Když označíme $[n] := \{1, 2, \dots n\}$, tak množina $\{[n] \mid n \in \mathbb{N}\} \subseteq \mathcal{P}(\mathbb{N})$ nemá maximální prvek. Všimněme si, že podobný protipříklad můžeme zkonstruovat pro libovolnou nekonečnou množinu.

Pozorování. *Množina x je konečná $\iff$ každá neprázdná $a \subseteq \mathcal{P}(x)$ má minimální prvek vůči inkluzi.*

Důkaz. Definujeme $d : \mathcal{P}(x) \to \mathcal{P}(x), u \mapsto x \setminus u$. Potom $u \subseteq v \Leftrightarrow d(u) \supseteq d(v)$. Klíčová úvaha: v je maximum množiny $a \subseteq \mathcal{P}(x) \iff d(v)$ je minimum množiny $d[a] = \{d(u) \mid u \in a\}$.

❑

Lemma 13. *Je-li x konečná a y nekonečná, potom $x \prec y$.*

Důkaz. Pro spor nechť $y \preceq x$, tedy existuje prosté zobrazení $f : y \to x$. Jelikož y je nekonečná, tak existuje $\varnothing \neq u \subseteq \mathcal{P}(y)$, která nemá maximální prvek vůči inkluzi. Definujme zobrazení $g : \mathcal{P}(y) \to \mathcal{P}(x)$ jako $g : a \mapsto f[a]$. Nyní množinu $u \subseteq \mathcal{P}(y)$ zobrazíme na množinu $g[u] \subseteq \mathcal{P}(x)$. Protože je x konečná, tak $g[u]$ má maximální prvek vůči inkluzi, označme jej m. Zobrazme nyní m pomocí g^{-1} zpátky do u, čímž získáme $n_0 := g^{-1}(m) \in u$. Jelikož u nemá maximální prvek vůči inkluzi, tak existuje $n_1 \in u$ t.ž. $n_0 \subset n_1$. Jelikož je f prostá, tak jsou g a g^{-1} také prosté, a proto $m = g(n_0) \subset g(n_1)$, což je spor s maximalitou m.

❑

Definice 41. Množina x je dedekindovsky konečná $\equiv (\forall y)(y \subset x \Rightarrow y \prec x)$.

Lemma 14. *Je-li x konečná, potom je i dedekindovsky konečná.*

Důkaz. Pro spor nechť pro nějaké $y \subset x$ platí $y \approx x$ a definujeme množinu všech takových zlobivých y jako

$$A \coloneqq \{y \subset x \,|\, y \approx x\}.$$

Protože $A \neq \varnothing$ a $A \subseteq \mathcal{P}(x)$, tak z konečnosti x existuje c, minimální prvek A vůči inkluzi. Protože $x \approx c$, tak existuje bijekce $f : x \to c$. Označme $d \coloneqq f[c]$. Protože $c \subset x$, tak $f[c] \subset f[x]$, tedy $d \subset c$. Jenže $f \restriction c$ je bijekce mezi c a d, tedy $c \approx d$, z čehož $d \approx x$, tedy $d \in A$. To je spor s minimalitou c.

❑

Poznámka. Opačná implikace nelze dokázat v ZF, potřebujeme AoC. V ZF dokonce existují dedekindovsky konečné množiny x, pro které je $\mathcal{P}(x)$ dedekindovsky nekonečná. Proto ta definice není moc šikovaná.

Poznámka. Další ekvivalentní definice konečnosti s Tarského. $\mathrm{Fin}(x) \iff$

- existuje lineární uspořádání '$\leq$' na x, které je dobré, a '$\geq$' je také dobré.
- existuje lineární uspořádání na x a každá dvě lin. usp. jsou izomorfní.
- $\mathcal{P}(\mathcal{P}(x))$ je dedekindovsky konečná.
- $(\exists n \in \omega)(x \approx n)$.

5.3.2 Vlastnosti uspořádání konečných množin

Lemma 15. *Je-li a konečná množina, uspořádaná relací $\leq$, potom má každá neprázdná $b \subseteq a$ minimální i maximální prvek vůči $\leq$.*

Důkaz. Maximalitu vůči $\leq$ převedeme na maximalitu vůči $\subseteq$. Máme $(a, \leq)$ a $\varnothing \neq b \subseteq a$. Pro každé $x \in b$ uvažme $(\leftarrow, x] \subseteq a$. Označme $u \coloneqq \{(\leftarrow, x] \,|\, x \in b\} \subseteq \mathcal{P}(a)$. Jelikož $u \neq \varnothing$ a a je konečná, tak u má minimální i maximální prvek vůči inkluzi. Všimněme si, že pokud je $(\leftarrow, m]$ maximální v u vzhledem k $\subseteq$, tak m je maximální v b vzhledem k $\leq$. Obdobně pro minimum.

❑

Věta 16. *Každé lineární uspořádání na konečné množině je dobré.*

Důkaz. Je to přímý důsledek: v lineárním uspořádání je minimální prvek automaticky i nejmenší.

❑

Definice 42 (Izomorfismus)**.** Nechť A_1, A_2 jsou třídy a R_1, R_2 relace. Bijekce $F : A_1 \to A_2$ je izomorfismus tříd A_1, A_2 vzhledem k relacím $R_1, R_2 \equiv$

$$(\forall x,y \in A_1)\big((x, y) \in R_1 \iff (F(x), F(y)) \in R_2\big).$$

Příklad. Speciálním případem izomorfismu je izomorfismus grafů. Tam jsou třídy A_1 a A_2 množiny vrcholů grafů G_1 a G_2, relace R_1 je relací „být hranou v G_1“ a R_2 je relací „být hranou v G_2“. Potom je bijekce $f : V_1 \to V_2$ izomorfismus grafů $G_1 = (V_1, E_1)$ a $G_2 = (V_2, E_2)$ právě tehdy, když

$$(\forall u,v \in V_1)\big((u, v) \in E_1 \iff (f(u), f(v)) \in E_2\big).$$

Izomorfismy se hodí i když hovoříme o uspořádáních. Řekneme, že F je počátkové vnoření A do B, je-li to izomorfismus nějakých dolních podmnožin A a B.

Definice 43 (Počátkové vnoření)**.** Nechť $(A, \leq_R)$ a $(B, \leq_S)$ jsou uspořádané množiny. Zobrazení F je počátkové vnoření A do $B \equiv$

1. $A_D \coloneqq \mathrm{Dom}(F) \subseteq A$ je dolní množina v A vůči $\leq_R$,
2. $B_D \coloneqq \mathrm{Rng}(F) \subseteq B$ je dolní množina v B vůči $\leq_S$.
3. F je izomorfismus A_D a B_D, vzhledem k R a S, tedy

$$(\forall a_1{,}a_2 \in A_D)(a_1 \leq_R a_2 \iff F(a_1) \leq_S F(a_2)),$$

Lemma 17. *Nechť F a G jsou počátková vnoření dobře uspořádané množiny $(A, \leq_R)$ do dobře uspořádané množiny $(B, \leq_S)$. Pak platí, že $F \subseteq G$ nebo $G \subseteq F$.*

Důkaz. Zřejmě $F, G \subseteq A \times B$, takže stačí dokázat, že $\mathrm{Dom}(F) \subseteq \mathrm{Dom}(G)$ a $\mathrm{Rng}(F) \subseteq \mathrm{Rng}(G)$; nebo naopak. Jelikož $\mathrm{Dom}(F)$ i $\mathrm{Dom}(G)$ jsou dolní množiny A a R je lineární, tak buď $\mathrm{Dom}(F) \subseteq \mathrm{Dom}(G)$, nebo naopak. BÚNO nechť $\mathrm{Dom}(F) \subseteq \mathrm{Dom}(G)$. Dokážeme

$$(\forall x \in \mathrm{Dom}(F))(F(x) = G(x)),$$

z čehož $\mathrm{Rng}(F) \subseteq \mathrm{Rng}(G)$. Pro spor nechť to neplatí a definujme

$$W \coloneqq \{x \in \mathrm{Dom}(F) \mid F(x) \neq G(x)\}.$$

Protože R je dobré, tak existuje $w \coloneqq \min_R(W)$. Jelikož $F(w) \neq G(w)$, tak z linearity S nastane buď $F(w) <_S G(w)$ nebo $G(w) <_S F(w)$, BÚNO nechť platí

$$F(w) <_S G(w). \tag{3}$$

Ukážeme, že $F(w) \notin \mathrm{Rng}(G)$, takže $\mathrm{Rng}(G)$ není dolní množina B, což je spor. Pro libovolné $z \in \mathrm{Dom}(G)$ nastane jedna ze dvou situací:

1. $z <_R w$, z čehož $G(z) <_S F(w)$, protože

$$\begin{aligned} G(z) &= F(z), && w \text{ je nejmenší, pro který se nerovnají} \\ F(z) &<_S F(w). && F \text{ je izomorfismus} \end{aligned}$$

2. $w \leq_R z$, z čehož $F(w) <_S G(z)$, protože

$$\begin{aligned} F(w) &<_S G(w), && \text{podle (3)} \\ G(w) &\leq_S G(z). && G \text{ je izomorfismus} \end{aligned}$$

V každém případě $F(w) \neq G(z)$, tedy $F(w) \notin \mathrm{Rng}(G)$.

❑

Věta 18 (O porovnávání dobrých uspořádání)**.** *Pokud jsou $(A, \leq_R)$ a $(B, \leq_S)$ dobře uspořádané množiny, tak existuje právě jedno zobrazení F, které je izomorfismem A a nějaké dolní podmnožiny B, nebo izomorfismem B a nějaké dolní podmnožiny A. Tedy minimálně jedna z těch množin se celá vyčerpá a F je počátkové vnoření.*

Důkaz. Označme P množinu všech počátkových vnoření A do B. Tvrdíme, že $F := \bigcup P$ je ten hledaný izomorfismus. Ověříme všechny podmínky:

1. F je zobrazení. Když $(x, y_1), (x, y_2) \in F$, tak existují počátková vnoření $F_1, F_2 \in P$ t.ž. $(x, y_1) \in F_1$ a $(x, y_2) \in F_2$. Podle lemmatu 17 platí $F_1 \subseteq F_2$ nebo $F_2 \subseteq F_1$. V každém případě jsou obě ty dvojce v alespoň jednom z F_1 nebo F_2, ale protože to jsou zobrazení, tak musí být $y_1 = y_2$.

2. F je prosté. Podobně, jenom využijeme, že F_1 a F_2 jsou počátková vnoření, tedy izomorfismy, tedy bijekce, takže jsou prosté, z čehož $x_1 = x_2$.

3. F je počátkové vnoření

   (a) $\mathrm{Dom}(F)$ je dolní množina v A. Nechť $x \in \mathrm{Dom}(F)$, $y \in A$ a $y <_R x$. Potřebujeme ukázat, že $y \in \mathrm{Dom}(F)$. Jelikož $x \in \mathrm{Dom}(F)$, tak existuje nějaké počátkové vnoření $F' \in P$ t.ž. $x \in \mathrm{Dom}(F')$. Protože $\mathrm{Dom}(F')$ je dolní množina, tak $y \in \mathrm{Dom}(F') \subseteq \mathrm{Dom}(F)$.

   (b) $\mathrm{Rng}(F)$ je dolní množina v B. Úplně stejná argumentace.

   (c) F je izomorfismus. Nejprve si uvědomme, že protože je F prosté, tak je to bijekce mezi množinami $\mathrm{Dom}(F)$ a $\mathrm{Rng}(F)$. Nyní nechť $x, y \in \mathrm{Dom}(F)$, potřebujeme aby
   $$x \leq_R y \iff F(x) \leq_S F(y).$$
   Opět musí existovat nějaké $F' \in P$ t.ž. $y \in \mathrm{Dom}(F')$. F' je počátkové vnoření, takže $\mathrm{Dom}(F')$ je dolní množina, tedy $x \in \mathrm{Dom}(F')$. Navíc, protože je F' izomorfismus, tak
   $$F(x) = F'(x) \leq_S F'(y) = F(y).$$

4. $\mathrm{Dom}(F) = A$ nebo $\mathrm{Rng}(F) = B$. Pro spor nechť $A \setminus \mathrm{Dom}(F)$ i $B \setminus \mathrm{Rng}(F)$ jsou neprázdné. Tedy mají nejmenší prvky a, b. Všimněme si, že $F' := F \cup \{(a, b)\}$ je také počátkové vnoření, tedy $F' \in P$, což je spor. Proč je to počátkové vnoření? Protože $\mathrm{Dom}(F)$ je dolní množina v A, tak všechny prvky v $A \setminus \mathrm{Dom}(F)$ musí být větší než všechno v $\mathrm{Dom}(F)$. Tedy a bude nový největší prvek v $\mathrm{Dom}(F')$. Podobně pro b a izomorfismus.

5. Jednoznačnost. Pro spor nechť existují dvě taková zobrazení $F_1 \neq F_2$. Podle lemmatu 17 nechť BÚNO $F_1 \subseteq F_2$. Protože $F_1 \neq F_2$, tak existuje nějaké $(a, b) \in F_2 \setminus F_1$. Jenže potom pro F_1 nemůže platit 4, což je spor. ❑

Věta 19. *Každá dvě lineární uspořádání na konečné množině jsou izomorfní.*

Důkaz. Nechť R, S jsou lineární uspořádání na konečné množině x. Protože x je konečná, tak díky větě 16 jsou to dokonce dobrá uspořádání. Máme tedy dvě dobře uspořádané množiny, $(x, \leq_R)$ a $(x, \leq_S)$. Podle předchozího lemmatu je množina $(x, \leq_R)$ izomorfní s nějakou dolní množinou $(a, \leq_S)$, kde $a \subseteq x$. Mohlo by to být i naopak, ale BÚNO uvažme tuto variantu. Chceme ukázat, že $x = a$. Pro spor nechť $a \subset x$. Jelikož se jedná o izomorfismus, tedy speciálně bijekci, tak $a \approx x$. Což ale znamená, že x není dedekindovsky konečná, a to je spor s lemmatem 14.

❑

5.3.3 Operace zachovávající konečnost

Lemma 20. *Platí*

1. $\mathrm{Fin}(x) \wedge y \subseteq x \implies \mathrm{Fin}(y)$,
2. $\mathrm{Fin}(x) \wedge y \approx x \implies \mathrm{Fin}(y)$,
3. $\mathrm{Fin}(x) \wedge y \preceq x \implies \mathrm{Fin}(y)$.

Důkaz.

1. Ukážeme, že libovolná $\varnothing \neq w \subseteq \mathcal{P}(y)$ má maximální prvek. To je jednoduché, protože $w \subseteq \mathcal{P}(y) \subseteq \mathcal{P}(x)$, tudíž $w \subseteq \mathcal{P}(x)$ a x je konečná.
2. Zřejmě $\mathcal{P}(x) \approx \mathcal{P}(y)$, dokonce jsou izomorfní vzhledem k $\subseteq$. Vynecháme detaily.
3. Plyne z předchozích dvou. Vezmeme nějakou $z \subseteq x$ t.ž. $z \approx y$.

❑

Lemma 21. *Sjednocení konečných množin je konečné:*

1. $\mathrm{Fin}(x) \wedge \mathrm{Fin}(y) \implies \mathrm{Fin}(x \cup y)$,
2. $\mathrm{Fin}(x) \implies (\forall y)\,\mathrm{Fin}(x \cup \{y\})$. *...triviální důsledek 1*

Důkaz. Nechť $\varnothing \neq w \subseteq \mathcal{P}(x \cup y)$, nalezneme maximální prvek. Idea je taková, že se zvlášť podíváme na x-ové a y-ové prvky množin ve w, najdeme maxima a zkombinujeme je. Definujme zobrazení

$$f_x : w \to \mathcal{P}(x) \qquad\qquad f_y : w \to \mathcal{P}(y)$$
$$u \mapsto u \cap x, \qquad\qquad u \mapsto u \cap y.$$

Potom označme

$$w_x \coloneqq \{f_x(u) \,|\, u \in w\}.$$

Zřejmě $\varnothing \neq w_x \subseteq \mathcal{P}(x)$, takže má maximální prvek vůči inkluzi, označme jej v_x. Nyní položme

$$w_y \coloneqq \{f_y(u) \,|\, u \in w \wedge f_x(u) = v_x\}.$$

Opět $\varnothing \neq w_y \subseteq \mathcal{P}(y)$, takže má maximální prvek v_y. Všimněme si, že $v_x \cup v_y$ je hledaný maximální prvek množiny w. Kdyby ne, tak by to byl spor s maximalitou v_x nebo v_y.

❑

5.3.4 Princip indukce pro konečné množiny

Definice 44. Definujeme třídu všech konečných množin $\mathrm{Fin} \coloneqq \{x \mid \mathrm{Fin}(x)\}$

Věta 22 (princip indukce pro konečné množiny)**.** *Je-li X třída, pro kterou platí*

1. $\varnothing \in X$,
2. $x \in X \Rightarrow (\forall y)(x \cup \{y\} \in X)$,

potom $\mathrm{Fin} \subseteq X$.

Důkaz. Pro spor nechť existuje nějaká množina $x \in \mathrm{Fin} \setminus X$. Definujme

$$w \coloneqq \{v \subseteq x \mid v \in X\}.$$

Podle 1 je $\varnothing \in w$, takže $\varnothing \neq w \subseteq \mathcal{P}(x)$. Protože je x konečná, tak w má maximální prvek vůči inkluzi, označme jej v_0. Tedy $v_0 \subseteq x$, ale $v_0 \neq x$, protože $v_0 \in X$. To znamená, že existuje nějaký prvek $y \in x \setminus v_0$. Položme $v_1 \coloneqq v_0 \cup \{y\}$. Podle 2 platí $v_1 \in w$, což je spor s maximalitou v_0.

❑

Lemma 23. $\mathrm{Fin}(x) \implies \mathrm{Fin}(\mathcal{P}(x))$.

Důkaz. Pomocí principu indukce. Ukážeme, že třída $X \coloneqq \{x \mid \mathrm{Fin}(\mathcal{P}(x))\}$ splňuje obě dvě podmínky, z čehož $\mathrm{Fin} \subseteq X$ a platí to pro všechny konečné množiny.

1. $\varnothing \in X$, protože $\mathcal{P}(\varnothing) = \{\varnothing\}$ je konečná množina.
2. Nechť $x \in X$ a y je libovolná množina, ukážeme $x \cup \{y\} \in X$. BÚNO $y \notin x$. Rozdělíme $\mathcal{P}(x \cup \{y\})$ na dvě části: $\mathcal{P}(x)$ a $z \coloneqq \mathcal{P}(x \cup \{y\}) \setminus \mathcal{P}(x)$. Všimněme si, že $\mathcal{P}(x) \approx z$ bijekcí $f : \mathcal{P}(x) \to z, u \mapsto u \cup \{y\}$. Z předpokladu je $\mathcal{P}(x)$ konečná, tedy z konečná také a sjednocení konečných množin je konečné, tedy $\mathcal{P}(x) \cup z = \mathcal{P}(x \cup \{y\})$ je konečná množina. ❑

Důsledek. $\mathrm{Fin}(x) \wedge \mathrm{Fin}(y) \implies \mathrm{Fin}(x \times y)$

Důkaz. $x \times y \subseteq \mathcal{P}(\mathcal{P}(x \cup y))$, jak jsme již ukázali v důkazu lemma 4.

❑

Lemma 24. *Sjednocení konečně mnoha konečných množin je konečná množina.*

$$\mathrm{Fin}(x) \wedge (\forall a \in x)\, \mathrm{Fin}(a) \implies \mathrm{Fin}\big(\bigcup x\big).$$

Důkaz. Pomocí principu indukce. Nechť $X = \{x \mid x \subseteq \mathrm{Fin} \wedge \mathrm{Fin}\big(\bigcup x\big)\}$.

1. $\varnothing \in X$, protože $\bigcup \varnothing = \varnothing$ a $\mathrm{Fin}(\varnothing)$.
2. Nechť $x \in X$, y je libovolná množina, ukážeme $x \cup \{y\} \in X$. Všimněme si, že
$$\bigcup(x \cup \{y\}) = y \cup \bigcup x.$$
Na pravé straně je sjednocení dvou konečných množin, což je konečná množina.

❑

Důsledek (Dirichletův princip pro nekonečné množiny)**.** *Je-li nekonečná množina sjednocením konečně mnoha množin, pak alespoň jedna z nich je nekonečná.*

V úvodu do této kapitoly jsme zmiňovali, že v ZF nelze dokázat, že relace $\preceq$ je trichotomická. Ovšem pro konečné množiny to lze pomocí indukce.

Lemma 25. *Každá konečná množina je srovnatelná se všemi množinami.*

$$\mathrm{Fin}(x) \implies (\forall y)(x \preceq y \vee y \preceq x).$$

Důkaz. Indukcí. Položme $X \coloneqq \{x \mid (\forall y)(x \preceq y \vee y \preceq x)\}$.

1. $\varnothing \in X$ protože $(\forall y) : \varnothing \subseteq y$, takže $\varnothing \preceq y$.
2. Nechť $x \in X$, u je libovolná množina a $z = x \cup \{u\}$. Chceme ukázat, že $z \in X$. BÚNO $u \notin x$. Nechť y je libovolná množina. Podle předpokladu je $x \preceq y$ nebo $y \preceq x$. Mohou nastat dvě možnosti:
   (a) $y \preceq x$, pak $y \preceq x \cup \{u\}$.
   (b) $x \prec y$, ukážeme $x \cup \{u\} \preceq y$. Nechť $f : x \mapsto y$ je prosté zobrazení x do y. Jelikož $x \prec y$, tak existuje $a \in y \setminus f[x]$. Definujme $g : x \cup \{u\} \to y$ jako $g \coloneqq f \cup (u, v)$. g je prosté zobrazení $x \cup \{u\}$ do y, tedy $x \cup \{u\} \preceq y$.

❑

Příklad. Pokud $\mathrm{Fin}(x)$ a $f : x \to y$, potom $\mathrm{Rng}(f) \preceq x$.

Příklad. Každou konečnou množinu lze dobře uspořádat.

5.4 Přirozená čísla a axiom nekonečna

Zermelo chtěl přirozená čísla definovat jako $0 \coloneqq \varnothing$ a $n \coloneqq \{n-1\}$. Russel a Frege zase jako $n \coloneqq \{x \mid x \text{ má } n \text{ prvků}\}$, to jsou ale vlastní třídy. Dnes se používá definice, kterou navrhl Von Neumann:

$$0 \coloneqq \varnothing, 1 \coloneqq \{0\}, 2 \coloneqq \{0,1\}, \ldots\ n+1 \coloneqq \{0,1,\ldots n\} = n \cup \{n\}.$$

Definice 45. Definujeme funkci následníka jako $S : V \to V$ jako $S : v \mapsto v \cup \{v\}$.

Definice 46. Množina w je induktivní, $\mathrm{Ind}(w) \equiv \varnothing \in w \wedge (\forall v \in w)(S(v) \in w)$.

Axiom (Nekonečna)**.** *Existuje nějaká induktivní množina, neboli* $(\exists x)\,\mathrm{Ind}(x)$.

Definice 47. Množina všech přirozených čísel je $\omega \coloneqq \bigcap\{w \mid \mathrm{Ind}(w)\}$.

Lemma 26. *ω je nejmenší induktivní množina.*

Důkaz. Pokud je w induktivní, tak $\varnothing \in w$, takže $\varnothing \in \omega$. Pokud $n \in \omega$, tak $(\forall w)(\mathrm{Ind}(w) \Rightarrow n \in w)$, tedy i $S(n) \in w$ a tudíž $S(n) \in \omega$.

❑

5.4.1 Princip indukce pro přirozená čísla

Věta 27. *Pokud $X \subseteq \omega$ a X je induktivní, potom $X = \omega$.*

Důkaz. Z definice ω platí $\omega \subseteq X$, tedy máme inkluzi v obou směrech. ❑

Důsledek. *Chceme dokázat $(\forall n \in \omega)\, \varphi(n)$, místo toho dokážeme*

$$\varphi(0), \qquad (\forall n \in \omega)\big(\varphi(n) \Rightarrow \varphi(S(n))\big).$$

Potom podle principu indukce platí $X := \{x \in \omega \mid \varphi(x)\} = \omega$.

Lemma 28 (o vlastnostech přirozených čísel)**.** *Pro libovolná $n, m \in \omega$ platí*

1. $n \in \omega \Rightarrow n \subseteq \omega$,
2. $m \in n \Rightarrow m \subseteq n$,
3. $n \notin n$.

Důkaz.

1. Dokážeme indukcí podle n. Pro nulu to platí, protože $0 \subseteq \omega$. Potom pro $n \in \omega$ už máme $n \subseteq \omega$. Protože $n \in \omega$, tak $\{n\} \subseteq \omega$ a i $n \cup \{n\} \subseteq \omega$
2. Indukcí podle n. Pro nulu to zjevně platí. Nyní nechť to platí pro n. Chceme ukázat, že pokud $m \in S(n)$, potom $m \subseteq S(n)$. Jelikož $m \in S(n) = n \cup \{n\}$, tak buď $m \in n$ a podle i.p. $m \subseteq n \subseteq S(n)$. Nebo $m = n \subseteq S(n)$.
3. Pro nulu to platí. Nyní nechť $n \in \omega$ a $n \notin n$. Pro spor předpokládejme, že $S(n) \in S(n) = n \cup \{n\}$. Potom buď $S(n) \in n$ nebo $S(n) = n$. V obou případech dostáváme inkluzi $S(n) \subseteq n$. Jenomže $S(n) = n \cup \{n\}$, takže $n \in n$ což je spor s i.p. ❑

5.4.2 Alternativní definice konečnosti

Lemma 29. *Každé přirozené číslo je konečná množina. Neboli $n \in \omega \Rightarrow \mathrm{Fin}(n)$.*

Důkaz. Indukcí. Zjevně $\mathrm{Fin}(0)$. Nyní nechť pro $n \in \omega$ platí $\mathrm{Fin}(n)$. Podle lemmatu o sjednocování konečných množin máme $\mathrm{Fin}(n \cup \{n\})$ ❑

Věta 30. *Množina x je konečná $\iff (\exists n \in \omega)(x \approx n)$.*

Důkaz. Směr '$\Leftarrow$' z lemmatu. Opačný směr indukcí pro konečné množiny. Definujeme množinu

$$X := \{x \mid (\exists n \in \omega)(x \approx n)\}.$$

Splníme předpoklady principu indukce, z čehož poplyne $\mathrm{Fin}(x) \Rightarrow x \in X$.

1. $\varnothing \in X$, protože $\varnothing \approx 0$.

2. Nechť $x \in X$ a y je množina. Chceme ukázat $x \cup \{y\} \in X$. Máme $x \approx n$ pro nějaké $n \in \omega$. BÚNO nechť $y \notin x$ (jinak $x \cup \{y\} = x \approx n$). Tvrdíme, že $x \cup \{y\} \approx S(n)$. Bijekci $f : x \to n$ rozšíříme o prvek (y, n), čímž získáme bijekci $g : x \cup \{y\} \to S(n)$. Tedy $x \cup \{y\} \approx S(n)$ a $x \cup \{y\} \in X$. ❑

Lemma 31. *ω je nekonečná.* *. . . všechny ostatní induktivní množiny také*

Důkaz. Musíme najít nějakou neprázdnou podmnožinu $\mathcal{P}(\omega)$, která nemá maximální prvek. Ukáže se, že to je samotná ω. Podle lemmatu o vlastnostech přirozených čísel pro každé $n \in \omega$ platí $n \subseteq \omega$, tedy $n \in \mathcal{P}(\omega)$, proto $\omega \subseteq \mathcal{P}(\omega)$. Zjevně $\omega \neq \emptyset$. Ukážeme, že nemá maximální prvek vůči inkluzi. Když $n \in \omega$, tak $n \subset n \cup \{n\} \in \omega$, tedy n není maximální. ❑

Lemma 32. *ω je dedekindovsky nekonečná.*

Důkaz. Musíme najít nějakou množinu $w \subset \omega$ t.ž. $w \approx \omega$. Vezmeme množinu $w := \omega \setminus \{0\}$. Naší bijekcí je funkce následníka $S : \omega \to w$. ❑

Poznámka. Jelikož každá konečná množina je ded. konečná, tak každý ded. nekonečná množina je nekonečná (obměna). Což je další důkaz nekonečnosti ω.

5.4.3 Uspořádání přirozených čísel relací náležení

Lemma 33. *Pro libovolná $n, m \in \omega$ platí*

$$m \in n \iff m \subset n$$

Důkaz. Směr '$\Rightarrow$' plyne z $m \subseteq n$ a $n \notin n$. Směr '$\Leftarrow$' indukcí podle n. Pro $n = 0$ nelze splnit předpoklad $m \subset 0$, takže to platí. Nyní nechť to platí pro nějaké $0 \neq n \in \omega$. Předpokládáme, že $m \subset S(n)$, budeme chtít ukázat, že $m \in S(n)$.

Ukážeme $m \subseteq n$, tedy buď $m \subset n$ a podle i.p. $m \in n$, nebo $m = n$, každopádně $m \in n \cup \{n\} = S(n)$.

Pro spor nechť $m \subset S(n) = n \cup \{n\}$, ale $m \nsubseteq n$. Potom musí být $n \in m$, tudíž podle lemmatu 28 $n \subseteq m$, takže $n \cup \{n\} = S(n) \subseteq m$, což je spor s $m \subset S(n)$. ❑

Lemma 34. *Relace $\in$ je lineární ostré uspořádání na ω. Neboli pro všechna $k, n, m \in \omega$ platí*

1. *$n \notin n$,* *. . . antireflexibilita*
2. *$m \in n \wedge n \in k \Rightarrow m \in k$,* *. . . tranzitivita*
3. *$m \in n \vee m = n \vee n \in m$.* *. . . trichotomie*

Důkaz.

1. Jak jsme dokázali v lemma 28.

2. Podle předchozího lemmatu lze relaci $\in$ zaměnit za $\subset$, což je tranzitivní. Šlo by to také přímo z vlastnosti $m \in n \Rightarrow m \subseteq n$, ale tohle je hezčí.

3. Pro pevně zvolené n to dokážeme indukcí podle m. Definujme množinu $X(n) \coloneqq \{m \in \omega \,|\, m \in n \vee m = n \vee n \in m\}$. Dokážeme, že $X(n)$ je induktivní a tedy $X(n) = \omega$. Nejprve uvažme $n = 0$. Určitě $0 \in X(0)$, protože $0 = 0$. Indukční krok: je-li $m \in X(0)$, tak buď $m = 0$ nebo $0 \in m$. Každopádně $0 \in m \cup \{m\} = S(m)$ a tedy $S(m) \in X(0)$. Z toho také vyplývá, že $(\forall n \in \omega)(0 \in X(n))$. Nyní zvolme $n \neq 0$ a $m \in X(n)$.

   (a) $m \in n$, takže podle předchozího lemmatu $m \subset n$. Také $\{m\} \subseteq n$, tedy $S(m) \subseteq n$. Pokud $S(m) = n$ tak jsme hotoví. Pokud $S(m) \subset n$, tak podle předchozího lemmatu $S(m) \in n$.

   (b) $m = n$ nebo $n \in m$. Každopádně $n \in m \cup \{m\} = S(m)$.

   Tedy $S(m) \in X(n)$ a $X(n) = \omega$.

❑

Věta 35. *ω je dobře ostře uspořádaná relací $\in$.*

Důkaz. Nechť $\varnothing \neq a \subseteq \omega$. Jelikož $\in$ je lineární na ω, tak nám stačí najít minimální prvek a (bude automaticky i nejmenší). Zvolme nějaké $n \in a$. Pokud je minimální, tak jsme vyhráli. Jinak nechť $b \coloneqq n \cap a$. Protože n je konečná, tak b je konečná (a neprázdná). Podle lemma 15 má b minimální prvek, označme jej m. Tvrdíme, že m je minimální i v a. Kdyby existovalo nějaké $x \in a$ t.ž. $x \in m$ (je menší než m), tak dojdeme ke sporu. Jelikož $m \in n$, tak $m \subseteq n$, tedy $x \in n$ a máme $x \in b$. Ale m je minimální v b.

❑

Úmluva. Běžně to budeme zkracovat: pokud o nějaké množině prohlásíme, že je „dobře uspořádaná relací $\in$“, tak tím myslíme, že je „dobře ostře uspořádaná relací $\in$“.

Další věta nám umožní poznat, kdy je něco uspořádané stejně jako ω.

Věta 36 (o charakterizaci uspořádání $\in$ na ω)**.** *Nechť A je nekonečná množina s ostrým lineárním uspořádáním '$<$' takovým, že pro každé $a \in A$ je množina $(\leftarrow, a]$ konečná. Potom je '$<$' dobré ostré uspořádání a navíc jsou uspořádané množiny $(A, <)$ a $(\omega, \in)$ izomorfní.*

Důkaz. První část je téměř stejná jako důkaz poslední věty.

1. '$<$' je dobré: Nechť $\varnothing \neq c \subseteq A$ a $a \in c$. Pokud a není minimální (nejmenší), tak označme $b \coloneqq c \cap (\leftarrow, a]$. Platí $a \in b$, takže $\varnothing \neq b \subseteq (\leftarrow, a]$. Podle předpokladu je b konečná, takže má minimální prvek m. Chceme ukázat, že m je minimální i v c. Pro spor nechť existuje nějaké $x \in c$ t.ž. $x < m$. Ukážeme, že $x \in b$, což bude spor. Protože $x < m < a$, tak $x \in (\leftarrow, a]$ a navíc $x \in c$, takže $x \in b$.

2. $(A, <)$ a $(\omega, \in)$ jsou izomorfní: podle věty 18 nastane jedna ze dvou možností:

(a) A je izomorfní s nějakou dolní množinou $B \subseteq \omega$. B není shora omezená, kdyby byla, tak $(\exists n)(\forall b \in B)(b \in n \vee b = n)$, takže $B \subseteq S(n)$, takže B by byla konečná, ale A je nekonečná, což je spor s $A \approx B$. Jelikož B není shora omezená, tak každé $n \in \omega$ je menší než nějaký prvek B a tedy $n \in B$, protože B je dolní množina. Tudíž $B = \omega$.

(b) ω je izomorfní s nějakou dolní množinou $C \subseteq A$. Opět C není omezená, stejným argumentem. A opět protože C je dolní množina, tak $C = A$.

❑

5.5 Různě velká nekonečna

Definice 48 (Spočetnost)**.** Množina x je

- spočetná $\equiv x \approx \omega$,
- nejvýše spočetná $\equiv$ je spočetná nebo konečná,
- nespočetná $\equiv$ není nejvýše spočetná.

5.5.1 Spočetné množiny

Věta 37. *Platí*

1. *každá shora omezená podmnožina $A \subseteq \omega$ je konečná,*
2. *každá shora neomezená podmnožina $A \subseteq \omega$ je spočetná.*

Důkaz.

1. A je shora omezená $n \in \omega$, pak $A \subseteq S(n)$, tedy $\mathrm{Fin}(A)$ ... viz minulý důkaz.
2. Je-li A konečná, tak má podle lemma 15 maximální (největší) prvek vůči $\in$, tedy je omezená. Obměna: A neomezená $\Rightarrow A$ nekonečná. Potřebujeme ale spočetnost. Použijeme poslední větu. A je nekonečná, lineárně uspořádaná relací $\in$ a pro každé n je $(\leftarrow, n] \subseteq S(n)$ konečná, tedy A a ω jsou izomorfní (vzhledem k $\in$), speciálně $A \approx \omega$.

❑

Důsledek. *Množina x je nejvýše spočetná $\iff x \preceq \omega$.*

Důsledek. *Každá podmnožina spočetné množiny je nejvýše spočetná.*

Důkaz. Nechť je A spočetná, f bijekce mezi A a ω, $B \subseteq A$, potom $B \approx f[B] \subseteq \omega$, tedy $B \preceq \omega$.

❑

Definice 49. Definujeme lexikografické (ostré) uspořádání $<_L$ na $\omega \times \omega$ jako

$$(m_1, n_1) <_L (m_2, n_2) \equiv (m_1 \in m_2 \vee (m_1 = m_2 \wedge n_1 \in n_2))$$

Intuice. Lex. ups. je dobré na $\omega \times \omega$. Prvky jsou vlastně uspořádané do mřížky, sloupečky jsou nekonečné stoupající řetězce a n-tý sloupeček je menší než $(n+1)$-ní sloupeček.

Příklad. Platí $\omega \times 2$ je izomorfní s ω – nekonečně sloupečků výšky dva. Ale $2 \times \omega$ není izomorfní s ω – dva nekonečné sloupečky. Všechno vůči $\in$.

Definice 50. Pro $m, n \in \omega$ definujme $\max(m, n) \coloneqq m$ pokud $n \in m$, jinak n. Maximo-lexikografické uspořádání na $\omega \times \omega$ definujeme jako

$$\begin{aligned}(m_1, n_1) <_{ML} (m_2, n_2) \equiv{} & \max(m_1, n_1) \in \max(m_2, n_2) \\ & \vee (\max(m_1, n_1) = \max(m_2, n_2) \wedge (m_1, n_1) <_L (m_2, n_2))\end{aligned}$$

Intuice. Procházíme jakoby čtverce/pravé úhly v nějaké vzdálenosti od počátku, a věci ve stejné vzdálenosti procházíme lexikograficky.

Příklad. Množina $(\omega \times \omega, <_{ML})$ je izomorfní s $(\omega, \in)$, tedy $\omega \times \omega \approx \omega$. Stačí ověřit, že $(\omega \times \omega, <_{ML})$ splňuje všechny předpoklady té charakterizační věty. Tenhle důkaz je hezký tím, že nepotřebujeme aritmetiku.

Ukážeme, že vyrobit ze spočetných množin nespočetnou množinu není jenom tak. Podobně jako konečné sjednocení nebo konečný součin konečných množin je konečný.

Věta 38. *Jsou-li A, B spočetné množiny, pak $A \cup B$ a $A \times B$ jsou také spočetné.*

Důkaz. Máme bijekce $f : A \to \omega$ a $g : B \to \omega$. Definujeme zobrazení $h : A \cup B \to \omega \times 2$ jako

$$h(x) \coloneqq \begin{cases} (f(x), 0), & \text{pro } x \in A, \\ (g(x), 1), & \text{jinak.} \end{cases}$$

Zobrazení h je prosté, ale nemusí to být bijekce. Takže $A \cup B \preceq \omega \times 2 \approx \omega$. Ale také $\omega \approx A \subseteq A \cup B$, takže $\omega \preceq A \cup B$ a podle Cantor-Bernsteinovy věty $A \cup B \approx \omega$.

Nyní pro $A \times B$. Definujeme $k : A \times B \to \omega \times \omega$ jako $k : (a, b) \mapsto (f(a), g(b))$. Protože je k bijekce, tak $A \times B \approx \omega \times \omega \approx \omega$.

❑

Důsledek. *Konečná sjednocení a konečné součiny spočetných množin jsou spočetné (indukcí).*

Důsledek. *Množiny $\mathbb{Z}$ a $\mathbb{Q}$ jsou spočetné. V sekci 5.2 jsme to dokázali pomocí aritmetiky, ovšem teď to umíme i bez ní.*

Důsledek (Dirichletův princip)**.** *Je-li nespočetná množina sjednocením konečně mnoha množin, tak alespoň jedna z nich je nespočetná.*

Dobrá, co kdybychom dělali sjednocení, resp. součin spočetně mnoha spočetných množin? Tyto pojmy si formálně definujeme až v kapitole o axiomu výběru, zatím je můžeme vnímat intuitivně. Ukážeme, že součin bude nespočetný, nehledě na platnost axiomu výběru. Spočetnost sjednocení nelze v ZF rozhodnout, ale ukážeme, že v ZFC bude sjednocení spočetné.

5.5.2 Cantorova věta

Věta 39 (Cantorova)**.** *Pro každou množinu x platí $x \prec \mathcal{P}(x)$.*

Důkaz. Zjevně $x \preceq \mathcal{P}(x)$, pomocí prostého zobrazení $f : x \to \mathcal{P}(x), a \mapsto \{a\}$. Pro spor předpokládejme, že existuje bijekce $f : x \to \mathcal{P}(x)$. Definujme množinu $T \coloneqq \{a \in x \mid a \notin f(a)\}$. Nyní pro každé $a \in x$ nastane jedna ze dvou situací:

$$
\begin{aligned}
a \in T &\implies a \notin f(a) \implies T \neq f(a), \\
a \notin T &\implies a \in f(a) \implies T \neq f(a).
\end{aligned}
$$

V každém případě $T \neq f(a)$, takže T nemá vzor, což je spor s tím, že f je bijekce. ❏

Důsledek. *Množina $\mathcal{P}(\omega)$ je nespočetná.*

Věta 40. *Univerzální třída V není množina.*

Důkaz. Kdyby byla, tak $V \prec \mathcal{P}(V)$. Ale určitě $\mathcal{P}(V) \preceq V$, což je spor. ❏

Důsledek. *Pro každé $n \geq 1$ je třída všech n-prvkových množin vlastní třídou.*

Důkaz. Kdyby byla množinou, tak z axiomu sumy by byla její suma také množina. Ale její suma je V. ❏

5.5.3 Kardinalita kontinua

Věta 41. ${}^{\omega}2 \approx \mathcal{P}(\omega) \approx \mathbb{R} \approx [0,1]$.

Důkaz. Podle lemma 9 platí $\mathcal{P}(\omega) \approx {}^{\omega}2$. Děláme charakteristické funkce posloupností: $\mathcal{P}(\omega) \to \{0,1\}$. Jako další ukážeme $[0,1] \approx {}^{\omega}2$.

1. $[0,1] \preceq {}^{\omega}2$. Číslo $a \in [0,1]$ zapíšeme binárně. Pokud $a = 0$, tak máme $0.000\ldots$ a pokud $a > 0$, tak $0.a_0a_1a_2\ldots$, kde nekonečmě mnoho a_i je 1 abychom odstranili duplicity pro periodická čísla. Takže třeba $0.5_{10} = 0.1_2$ zapíšeme jako $0.0111\ldots$. Tyto nekonečné posloupnosti jsou zjevně funkce z ω do $\{0,1\}$.

2. ${}^{\omega}2 \preceq [0,1]$. Problém je, že posloupnosti $0.1000\ldots$ a $0.0111\ldots$ se zobrazí na stejné reálné číslo. Ale kdybychom to četli ve trojkové soustavě, tak už to budou různá čísla. Proto defingujeme funkci $f : {}^{\omega}2 \to [0,1]$ jako

$$
f : (a_0, a_1, a_2, \ldots) \mapsto \sum_{i=0}^{\infty} \frac{a_i}{3^{i+1}}.
$$

Tedy podle Cantor-Bernsteinovy věty $\mathcal{P}(\omega) \approx {}^\omega 2 \approx [0,1]$. Zbývá ukázat $[0,1] \approx \mathbb{R}$. Zřejmě $[0,1] \preceq \mathbb{R}$, protože $[0,1] \subseteq \mathbb{R}$. Opačně $\mathbb{R} \preceq [0,1]$ například prostou funkcí

$$\arctan : \mathbb{R} \mapsto (-\pi/2, \pi/2),$$

kterou vhodně upravíme, aby se to zobrazilo na $(0,1)$. Ukázat $[0,1] \approx (0,1)$ už je snadné.

❑

Ukázali jsme, že reálných čísel je více než přirozených. Je přirozené položit si otázku, zda existuje něco mezi? Bylo by hezké, kdyby nejmenší množina, větší než přirozená čísla, byla reálná přímka (kontinuum). Tato myšlenka se nazývá hypotéza kontinua, anglicky Continuum hypothesis (CH). Formuloval ji už Cantor a říká, že neexistuje žádná množina x taková, že

$$\omega \prec x \prec \mathcal{P}(\omega) \approx \mathbb{R}.$$

Tedy každá $x \subseteq \mathbb{R}$ je buď spočetná, nebo ekvivalentní s $\mathbb{R}$. Gödel (1940) dokázal, že CH nelze v ZFC vyvrátit. Cohen (1963) dokázal, že nelze v ZFC dokázat. Tedy je možné k ZFC bezesporně přidat jako axiom CH i $\neg$CH.

5.5.4 Algebraická čísla

Algebraická čísla jsou kořeny polynomů s celočíselnými koeficienty. Takže například $\sqrt{2}$ je algebraické číslo, protože je kořenem polynomu $x^2 - 2$. Čísla, která nejsou algebraická nazýváme transcendentní.

Fakt. *Je-li A spočetná množina, potom*

1. *množina všech konečných podmnožin A je spočetná,*
2. *množina všech konečných posloupností prvků množiny A je spočetná.*

Tvrzení 42. *Algebraických čísel je spočetně mnoho.*

Důkaz. Polynom odpovídá nějaké konečné posloupnosti $(a_0, a_1, \dots a_n)$ celých čísel. Celých čísel je spočetně mnoho, takže těchto posloupností je také spočetně mnoho.

Tedy každému polynomu přiřadíme nějaké pořadové číslo. Navíc víme, že polynom stupně n má nejvýše n kořenů. Algebraických čísel je určitě alespoň spočetně mnoho, musíme ukázat, že jich není víc. Proto definujeme prosté zobrazení všech algebraických čísel do spočetné množiny $\omega \times \omega$. Každý reálný kořen x polynomu

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0, \qquad a_0 \neq 0$$

je jednoznačně určen dvojicí (k, l), kde k je číslo přiřazené posloupnosti koeficientů tohoto polynomu a l udává, že x je l-tý reálný kořen tohoto polynomu podle velikosti. Ovšem jednomu algebraickému číslu může odpovídat víc dvojic (k, l), stačí rovnici vynásobit nějakou konstantou. Proto algebraickému číslu x přiřadíme ze všech dvojic (k, l), které mu odpovídají, tu nejmenší vzhledem k maximo-lexikografickému uspořádání.

❑

Důsledek. *Transcendentních čísel je nespočetně mnoho.*

6 Axiom výběru

Axiom výběru, anglicky Axiom of choice (Aoc), má mnoho důležitých důsledků a je klíčový v mnoha oblastech matematiky, například v analýze a lineární algebře. Bez něj nelze dokázat spousta tvrzení, která by intuitivně měla platit. Jeho přidáním do Zermelova–Fraenkelovy teorie množin získáme teorii ZFC.

Nicméně axiom výběru je také kontroverzní, protože některé jeho důsledky odporují intuici, jako například princip dobrého uspořádání, který říká, že každou množinu lze dobře uspořádat. Nebo Banach-Tarski paradox, který uvádí postup, jak rozdělit kouli na konečný počet částí a tyto části přeskupit tak, aby vznikly dvě koule identické s tou původní.

6.1 Indexované soubory množin

Definice 51. Soubor množin $\langle X_i \mid i \in I \rangle$ je zobrazení F s definičním oborem I, kde X_i označuje množinu $F(i)$. Říkáme, že I je indexová třída tohoto souboru a že x patří do souboru, jestliže pro nějaké $i \in I$ platí $x = X_i$. Definujeme

$$\bigcup_{i\in I} X_i \coloneqq \bigcup \mathrm{Rng}(F),$$
$$\bigcap_{i\in I} X_i \coloneqq \bigcap \mathrm{Rng}(F),$$
$$\prod_{i\in I} X_i \coloneqq \{f \mid f : I \mapsto \bigcup_{i\in I} X_i \wedge (\forall i \in I)(f(i) \in X_i\}.$$

Definice kartézského součinu má smysl jen pro soubory indexované množinou, protože vlastní třídy nebohou nikam náležet.

Lemma 43. *Je-li I množina a $\langle X_i \mid i \in I \rangle$ soubor indexovaný I, potom jsou třídy $\bigcup_{i\in I} X_i$, $\bigcap_{i\in I} X_i$ a $\prod_{i\in I} X_i$ také množinami.*

Důkaz. $\mathrm{Dom}(F) = I$ je množina, takže podle axiomu nahrazení je $\mathrm{Rng}(F) = F[I]$ také množina. Proto jsou suma a průnik také množiny. Všimněme si, že produkt je podmnožinou množiny všech zobrazení z I do $\bigcup_{i\in I} X_i$, což je množina.

❑

Pozorování. *Pokud pro každé $i \in I$ je $X_i = X$, tak $\prod_{i\in I} X_i = {}^I X$.*

Lemma 44. *Je-li $\langle X_i \mid i \in \omega \rangle$ spočetný soubor množin, kde na každém X_i existuje dobré uspořádání a $2 \preceq X_i$, potom je součin tohoto souboru nespočetný.*

Důkaz. Není těžké ukázat, že

$$\prod_{i\in\omega} 2 \preceq \prod_{i\in\omega} X_i.$$

Podle posledního pozorování ovšem platí $\prod_{i\in\omega} 2 = {}^\omega 2 \approx \mathcal{P}(\omega)$, což je podle Cantorovy věty nespočetná množina.

❑

Důsledek. *Kartézský součin spočetně mnoha spočetných množin je nespočetný.*

6.2 Co axiom výběru tvrdí

Ukažme si motivaci za zavedením axiomu výběru. Mějme f, zobrazení množiny X na množinu Y a podívejme se na rozklad množiny X definovaný jako

$$r := \{f^{-1}[y] \mid y \in Y\}.$$

Existuje prosté zobrazení $g : Y \to X$?

- Pro konečné Y lze dokázat indukcí. Neformálně si prostě konečně-mnohokrát vezmu nějaký prvek z $f^{-1}[y]$.
- Pro dobře uspořádané X vezmu z $f^{-1}[y]$ vždy ten nejmenší prvek.
- Obecně to v ZF dokázat nelze – museli bychom pro každé $y \in Y$ vybrat nějakého reprezentanta $x \in f^{-1}[y]$ z potenciálně nekonečné množiny, ale těch $y \in Y$ taky může být nekonečně mnoho.

Původní formulace axiomu výběru zněla následovně.

Princip (Výběru)**.** *Pro rozklad r množiny X existuje výběrová množina $v \subseteq X$ t.ž $(\forall u \in r)(\exists x)(v \cap u = \{x\})$. Takže z každé rozkladové třídy vybereme jednoho reprezentanta.*

Dnes se ovšem používá poněkud šikovnější formulace přes selektory.

Definice 52 (Selektor)**.** Je-li R množina, pak funkci $f : R \to \bigcup R$ splňující

$$(\forall t \in R)(t \neq \varnothing \Rightarrow f(t) \in t),$$

nazýváme selektor na množině R. BÚNO můžeme předpokládat, že selektor je definovaný na množině $R \setminus \{\varnothing\}$ a pro každé $t \in \mathrm{Dom}(R)$ platí $f(t) \in t$.

Axiom 10 (Výběru)**.** *Na každé množině existuje selektor.*

Věta 45. *Tvrzení ekvivalentní s AoC:* [1]

- *Princip dobrého uspořádání – každou množinu lze dobře uspořádat.*
- *Princip trichotomie – relace $\preceq$ je trichotomická.*
- *Princip maximality, také známý jako Zornovo lemma.*

Trochu slabší důsledky:

- *Každý vektorový prostor má bázi.*
- *Součin kompaktních prostorů je kompaktní.*
- *Princip kompaktnosti z kombinatoriky. Příklad použití: graf je 3-obarvitelný $\Leftrightarrow$ každý jeho konečný podgraf je 3-obarvitelný.*
- *Banach-Tarski paradox.*

[1] "The Axiom of Choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn's lemma?" — Jerry Bona

Všechna tato tvrzení lze dokázat bez AoC, pokud uvažujeme pouze konečné případy.

Lemma 46. *Následující tvrzení jsou ekvivalentní:*

1. *axiom výběru,*
2. *princip výběru,*
3. *pro každou množinovou relaci s existuje funkce $f \subseteq s$ t.ž.* $\mathrm{Dom}(f) = \mathrm{Dom}(s)$,
4. *kartézský součin $\prod_{i\in I} X_i$ neprázdného souboru neprázdných množin je neprázdný.*

Důkaz.

$1 \Rightarrow 2$ Nechť r je rozklad X, podle axiomu výběru existuje selektor f na r. Hledaná výběrová množina je $\mathrm{Rng}(f)$.

$2 \Rightarrow 3$ Pokud $s = \varnothing$, potom $f = \varnothing$ a není co dokazovat. Proto nechť $s \neq \varnothing$. Definujeme rozklad r množiny s jako

$$r := \big\{\{(x, y) \in s \,|\, y \in \mathrm{Rng}(s)\} \,|\, x \in \mathrm{Rng}(s)\big\}.$$

Podle principu výběru existuje výběrová množina tohoto rozkladu, což je právě hledaná funkce f.

$3 \Rightarrow 4$ Neprázdný soubor neprázdných množin $\big\langle X_i \,|\, i \in I\big\rangle$ určuje relaci $s := \{(i,x) \,|\, i \in I \wedge x \in X_i\}$. Podle 3 existuje funkce $f \subseteq s$ t.ž. $\mathrm{Dom}(f) = \mathrm{Dom}(s) = I$ a tedy f je prvkem uvažovaného produktu.

$4 \Rightarrow 1$ Nechť x je libovolná množina, musíme ukázat, že na ní existuje selektor. BÚNO předpokládejme, že $x \neq \varnothing$ a $\varnothing \notin x$. Identita na x určuje neprázdný soubor neprázdných množin $\big\langle y \,|\, y \in x\big\rangle$, který má podle 4 neprázdný kartézský součin. Všimněme si, že každý prvek tohoto součinu je selektor na x. ❑

Lemma 47. *AoC $\Longrightarrow$ Sjednocení spočetného souboru (nejvýše) spočetných množin je (nejvýše) spočetné.*

Důkaz. Uvažme soubor $\big\langle B_i \,|\, i \in I\big\rangle$, BÚNO $I = \omega$. Sestrojíme prosté zobrazení z $S := \bigcup_{i\in\omega} B_i$ do $\omega \times \omega$. Nechť E_i je množina všech prostých zobrazení $f : B_i \to \omega$, ze spočetnosti B_i je $E_i \neq \varnothing$, a definujeme soubor $\big\langle E_i \,|\, i \in \omega\big\rangle$. Podle posledního lemmatu je produkt tohoto souboru neprázdný, existuje tedy soubor $\big\langle f_i \,|\, i \in \omega\big\rangle$, kde $f_i \in E_i$. Definujeme $h : S \to \omega \times \omega$ jako $h : b \mapsto (i, f_i(b))$, kde i je nejmenší index z ω, že $b \in B_i$. ❑

Poznámka. Bez AoC lze bezesporně předpokládat, že nespočetná množina $\mathbb{R}$ je sjednocením spočetně mnoha spočetných množin.

6.3 Princip maximality

Axiom výběru je ekvivalentní s řadou tvrzení, jedno z nejpoužívanějších je Zornovo lemma, také známé jako princip maximality. Důkaz ekvivalence vynecháme.

Definice 53 (Řetězec)**.** Nechť $(A, \leq)$ je uspořádaná množina. Podmnožinu $B \subseteq A$ nazveme řetězcem v A, je-li B lineárně uspořádaná relací $\leq$.

Princip (Maximality (PM))**.** *Nechť $(A, \leq)$ je uspořádaná množina, kde každý řetězec je shora omezený. Potom pro každé $a \in A$ existuje maximální prvek b množiny A t.ž. $a \leq b$.*

Poznámka. Často se používá pro uspořádání $(A \subseteq)$, kde $A \subseteq \mathcal{P}(x)$. Pak pro řetězec $B \subseteq A$ stačí ukázat, že $\bigcup B \in A \ldots \bigcup B \in A$ je totiž horní mez B vzhledem k $\subseteq$.

Princip (Maximality II (PMS))**.** *Nechť $(A, \leq)$ je uspořádaná množina, kde každý řetězec má supremum. Potom pro každé $a \in A$ existuje maximální prvek b množiny A t.ž. $a \leq b$.*

Příklad. Dokažte (PM) $\iff$ (PMS).

Přechodem k inverznímu uspořádání dostáváme z principu maximality princip minimality.

Princip (Minimality)**.** *Nechť $(A, \leq)$ je uspořádaná množina, kde každý řetězec je zdola omezený. Potom pro každé $a \in A$ existuje minimální prvek b množiny A t.ž. $b \leq a$.*

6.4 Princip trichotomie

Princip (Trichotomie)**.** *Pro libovolné množiny x, y platí $x \preceq y$ nebo $y \preceq x$.*

Lemma 48. *Princip maximality $\implies$ princip trichotomie.*

Důkaz. Nejprve si připomeňme, že inverzní zobrazení k prostému zobrazení je prosté. Nyní nechť x, y jsou množiny, chceme sestrojit prosté zobrazení x do y, nebo y do x. Definujme množinu

$$P \coloneqq \{f \mid f \text{ je prosté zobrazení} \wedge \mathrm{Dom}(f) \subseteq x \wedge \mathrm{Rng}(f) \subseteq y\}.$$

Všimněme si, že uspořádaná množina $(D, \subseteq)$ splňuje podmínky principu maximality, jelikož sjednocení řetězce prostých zobrazení je prosté zobrazení. Nechť g je nějaký maximální prvek P. Kdyby obě množiny $x \setminus \mathrm{Dom}(g)$ a $y \setminus \mathrm{Rng}(g)$ byly neprázdné, tak by g šlo rozšířit o další dvojici, což je spor s maximalitou g. Proto buď $\mathrm{Dom}(g) = x$ a potom $x \preceq y$, nebo $\mathrm{Rng}(g) = y$ a potom $y \preceq x$.

❑

Lemma 49. *AoC $\implies$ ω je nejmenší nekonečná množina.*

Důkaz. Je-li x spočetná, tak $\omega \approx x$. Je-li nespočetná, tak z trichotomie buď $\omega \preceq x$ nebo $x \preceq \omega$. Jelikož x není spočetná ani konečná, tak druhá varianta nenastane.

❑

Důsledek. *Množina x je konečná $\iff$ je dedekindovsky konečná.*

Důkaz. V ZF jsme dokázali, že každá konečná množina je ded. konečná. Z toho obměnou, že každá ded. nekonečná je nekonečná. Nyní ukážeme, že každá nekonečná je ded. nekonečná. Z předchozího lemma víme, že pokud je x nekonečná, tak $\omega \preceq x$ z lemma 32, že ω je ded. nekonečná. Není těžké ukázat, že x musí být také ded. nekonečná.

❑

6.5 Princip dobrého uspořádání

Princip (Dobrého uspořádání (W-O))**.** *Každou množinu lze dobře uspořádat.*

Lemma 50. *Well-ordering principle $\implies$ axiom výběru*

Důkaz. Nechť x je množina splňující $x \neq \varnothing$ a $\varnothing \notin x$. Chceme sestrojit selektor $f : x \to \bigcup x$. Ten musí splnit $(\forall y \in x) : f(y) \in y$. Podle W-O existuje dobré uspořádání $\leq$ na $\bigcup x$ a každá $y \in x$ je neprázdná podmnožina $\bigcup x$, tedy má nejmenší prvek vůči $\leq$. Selektor f definujeme jako $f : y \mapsto \min_{\leq}(y)$.

❑

Příklad. Dokažte (PM) $\implies$ (W-O).

7 Ordinální čísla

Ordinální čísla jsou zobecnění přirozených čísel a udávají typy dobře uspořádaných množin. Pomocí ordinálních čísel pak lze nadefinovat kardinální čísla, což jsou speciální ordinální čísla, která měří mohutnosti množin. Ordinální čísla definujeme tak, aby byla dobře uspořádána relací $\in$, takže na nich budeme moci provádět takzvanou transfinitní indukci.

7.1 Tranzitivní třídy

Definice 54. Třída X je tranzitivní $\equiv y \in x \in X \Rightarrow y \in X$.

Pozorování. *Ekvivalentně:* $x \in X \Rightarrow x \subseteq X$.

Pozorování. X *je tranzitivní* $\iff \bigcup X \subseteq X$.

Lemma 51. *Vlastnosti tranzitivních tříd.*

1. *Jsou-li* X, Y *tranzitivní třídy, pak* $X \cap Y$ *a* $X \cup Y$ *jsou také tranzitivní.*

2. *Jsou-li všechny prvky* $x \in X$ *třídy* X *tranzitivní, tak* $\bigcap X$ *a* $\bigcup X$ *jsou také tranzitivní.*

3. *Je-li* X *tranzitivní třída, pak relace* $\in$ *je tranzitivní na* $X \iff$ *každé* $x \in X$ *je tranzitivní množina.*

Důkaz.

1. Plyne přímo z definice.

2. Ukážeme pro průnik, suma podobně. Nechť $y \in z \in \bigcap X$, chceme ukázat $y \in \bigcap X$. Protože je každá $x \in X$ tranzitivní, tak z $y \in z \in x$ máme $y \in x$, tedy $y \in \bigcap X$ a X je tranzitivní.

3. Nejprve '$\Rightarrow$'. Je-li $\in$ tranzitivní na X a $z \in y \in x \in X$, tak $z \in x$, tedy x je tranzitivní množina. Nyní '$\Leftarrow$'. Je-li každé $x \in X$ tranzitivní a $z \in y \in x \in X$, tak z tranzitivity x je $y \in X$ a z tranzitivity y je $z \in x$, tedy relace $\in$ je tranzitivní na X.

❑

7.2 Uspořádání ordinálních čísel relací náležení

Definice 55. Množina x je ordinální číslo $\equiv$

1. x je tranzitivní,

2. relace $\in$ je dobré ostré uspořádání na x.

Třídu všech ordinální čísel značíme O_n

Poznámka. Každé $n \in \omega$ i samotné ω jsou ordinální čísla.

Lemma 52. *Třída* O_n *je tranzitivní.*

Důkaz. Ukážeme, že každé $y \in x \in O_n$ je také ordinální číslo, tedy $y \in O_n$. Protože x je ordinál, tak relace $\in$ je na x dobré uspořádání, speciálně je tedy tranzitivní. Podle třetí části lemma 51 je potom $y \in x$ tranzitivní množina. Ještě musíme ukázat, že $\in$ je dobré uspořádání na y. Ale to je, jelikož $y \in x \Rightarrow y \subseteq x$ a relace „být dobré uspořádání“ je dědičná (x je dobře uspořádaná, protože to je ordinál).

❑

Lemma 53. *Relace $\in$ je tranzitivní na O_n.*

Důkaz. Ukázali jsme, že O_n je tranzitivní a navíc každé $x \in O_n$ je tranzitivní, takže podle třetí části lemma 51 je relace $\in$ tranzitivní na O_n.

❑

Lemma 54. *Pro každá dvě $x, y \in O_n$ platí*

1. $x \notin x$,
2. $x \cap y \in O_n$,
3. $x \in y \iff x \subset y$.

Důkaz.

1. Z antireflexibility $\in$ na x.
2. Podle lemma 51 je $x \cap y$ tranzitivní množina a je dobře uspořádaná relací $\in$, protože to je podmnožinou ordinálu x.
3. Směr '$\Rightarrow$' z tranzitivity y a 1. Pro opačný směr nechť $x \subset y$. Protože y je dobře uspořádaná, tak $\varnothing \neq y \setminus x \subseteq y$ má nejmenší prvek vůči $\in$, označme jej z. Ukážeme, že $z = x$. Nejprve inkluze $x \subseteq z$. Nechť $u \in x$, protože $x \subseteq y$, tak $u \in y$. Protože y je ordinál, tak $\in$ je lineární na y, tedy u můžeme porovnat se z. Jsou tři možnosti

   (a) $u \in z$, to jsme chtěli,
   (b) $u = z$, ale $z \notin x$, takže $u \notin x$, což je spor,
   (c) $z \in u$, z tranzitivity x máme $z \in u \in x \implies z \in x$, což je opět spor.

   Nyní inkluze $z \subseteq x$. Nechť $u \in z$, podle tranzitivity y máme $u \in z \in y \implies u \in y$, ukážeme $u \in x$. Kdyby $u \notin x$, tak u je menší prvek v doplňku $y \setminus x$ než z, což je spor s minimalitou z.

❑

Věta 55. *Relace $\in$ je dobré (ostré) uspořádání na O_n.*

Důkaz. Je tranzitivní a antireflexivní, takže to je ostré uspořádání.

1. Trichotomie (a z toho linearita). Nechť $x, y \in O_n$, chceme je porovnat. Podívejme se na množinu $z := x \cap y \in O_n$. Ukážeme, že $z = x$ nebo $z = y$. Kdyby $z \subset x$ a $z \subset y$, pak podle minulého lemmatu $z \in x$ a $z \in y$, čili $z \in z$, což je spor. Nyní rozbor případů:

   (a) $x = y$, pak jsme skončili,
   (b) $z = x \wedge z \subset y$, pak $x \in y$ ... podle předchozího lemmatu,
   (c) $z = y \wedge z \subset x$, pak $y \in x$ ... podle předchozího lemmatu.

2. Dobrost dokážeme podobně jako pro ω. Nechť $A \subseteq O_n$ je nepřázdá a $\alpha \in A$. Není-li α minimální, označme $b := \alpha \cap A$. BÚNO $b \neq \varnothing$, jinak by bylo minimální. Jelikož $b \subseteq \alpha$ a α je ordinální číslo, tak je b dobře uspořádané a má nejmenší prvek β (vůči $\in$). Tvrdíme, že β je minimální v A. Kdyby ne, tak existuje nějaké $\gamma \in \beta$ t.ž. $\gamma \in A$. Ale $\beta \in \alpha$, takže z tranzitivity α je $\gamma \in \alpha$. Tedy $\gamma \in b$, což je spor s minimalitou β. ❑

Důsledek. *Třída O_n není množina.*

Důkaz. Ukázali jsme, že O_n je tranzitivní a $\in$ je na ní dobré ostré uspořádání, tedy kdyby to byla množina, tak je to ordinál, tedy $O_n \in O_n$, což je spor. ❑

Důsledek. *Je-li X tranzitivní vlastní třída dobře uspořádaná relací $\in$, pak $X = O_n$.*

Důkaz. Jelikož je X tranzitivní, tak pokud $x \in X$, potom $x \subseteq X$. Protože X je dobře uspořádaná relací $\in$, tak z dědičnosti je x také dobře uspořádaná. Navíc jelikož je $\in$ tranzitivní na X, tak x je tranzitivní množina. Proto je x ordinální číslo, čili $X \subseteq O_n$. Pro spor nechť platí pouze ostrá inkluze a $x \in O_n \setminus X$. Ukážeme, že $X \subseteq x$, což je spor s tím, že X je vlastní třída.

Nechť $y \in X$, kdyby $y \notin x$, tak z trichotomie $\in$ na O_n musí být $x \in y$. Z tranzitivity X bychom pak měli $x \in X$, což je spor. ❑

7.3 Vlastnosti ordinálních čísel

Úmluva. Ordinální čísla značíme řeckými písmeny α, β, γ, píšeme $\alpha < \beta$ namísto $\alpha \in \beta$ a $\alpha \leq \beta$ namísto $\alpha \in \beta \vee \alpha = \beta$.

Lemma 56. *Pro ordinální čísla platí následující.*

1. *Nechť $x \subseteq O_n$ je množina. Pak x je ordinální číslo $\iff$ x je tranzitivní.*
2. *Nechť $\varnothing \neq A \subseteq O_n$ je třída. Pak $\bigcap A$ je nejmenší prvek A (vzhledem k $<$).*
3. *Nechť $A \subseteq O_n$ je množina, pak $\bigcup A$ je ordinální číslo a dokonce to je supremum A.*

Důkaz.

1. Směr '$\Rightarrow$' z definice. Pro opačný směr nechť x je tranzitivní, potřebujeme aby $\in$ bylo dobré uspořádání na x. Ale podle předchozí věty je $\in$ dobré uspořádání na O_n, takže z dědičnosti i na $x \subseteq O_n$.

2. Podle předchozí věty má A nejmenší prvek α, ukážeme $\alpha = \bigcap A$. Pro libovolné $\beta \in A$ platí $\alpha \leq \beta$. Buď $\beta = \alpha$ nebo $\alpha \in \beta$, protože ordinály jsou tranzitivní, tak $\alpha \subseteq \beta$. Každopádně $\alpha \subseteq \beta$, proto $\alpha = \bigcap A$.

3. Podle lemma 51 je $\bigcup A$ tranzitivní, protože všechny prvky A jsou tranzitivní. Jelikož to je tranzitivní množina ordinálních čísel, tak podle 1 je to ordinál. Teď ještě musíme ukázat, že to je supremum A. Nejprve, že to je horní mez. Nechť $\alpha \in A$, potom $\alpha \subseteq \bigcup A =: \beta$. Pokud $\alpha = \beta$, tak jsme skončili. Pokud $\alpha \subset \beta$, tak podle lemma 54 je $\alpha \in \beta$. Každopádně $\alpha \leq \beta$, tedy β je horní mez množiny A. Nyní ukážeme, že žádné $\gamma < \beta$ horní mez být nemůže. Pokud $\gamma < \beta$, neboli $\gamma \in \bigcup A$, tak existuji $\alpha \in A$ t.ž. $\gamma \in \alpha$, neboli $\gamma < \alpha$, tedy γ není horní mezí A. ❑

Důsledek. *Ordinál ω je supremum množiny všech přirozených čísel v O_n. To znamená, že ω je nejmenší nekonečné ordinální číslo. Konečné ordinály jsou právě přirozená čísla.*

Důkaz. Podle lemma je $\sup(\omega) = \bigcup \omega$ a není těžké ukázat, že $\bigcup \omega = \omega$. Je-li x nekonečné ordinální číslo, tak $\omega \preceq x$, jak jsme dokázali v kapitole o AoC. Je-li x konečné, tak z trichotomie nastane jeden ze tří případů:

1. $x < \omega$, neboli $x \in \omega$, tedy x je přirozené číslo,

2. $x = \omega$, ale to je spor s konečností x,

3. $x > \omega$, neboli $\omega \in x$, ale protože x je ordinál, tak je tranzitivní, tedy $\omega \subseteq x$, což je spor s konečností x. ❑

7.4 Typy dobře uspořádaných množin

Jsou-li dvě množinové relace izomorfní, tak se podstatně neliší, přestože popisují vztahy mezi prvky různých množin. Dává proto smysl uvažovat ekvivalenci „být izomorfní“ na třídě všech relací. Je snadné nahlédnout, že ekvivalenční třídy této relace jsou vlastní třídy, proto nemůžeme udělat rozklad. Ale bylo by hezké, kdybychom mohli pro každou ekvivalenční třídu sestrojit nějakého reprezentanta, abychom pak mohli vše týkající se relací daného typu dokazovat na tomto reprezentantovi. Tito reprezentanti jsou právě ordinální čísla.

Věta 57 (O typu dobrého uspořádání)**.** *Je-li a množina dobře uspořádaná relací R, pak existuje právě jedno ordinální číslo α a jednoznačně určený izomorfismus $(a, \leq_R)$ a $(\alpha, <)$. Ordinálnímu číslu α říkáme typ uspořádané množiny $(a, \leq_R)$.*

Poznámka. Tohle byla původní Cantorova definice ordinálních čísel. Ta naše je Von-Neumannova.

7.5 Princip transfinitní indukce

Lemma 58. *Pokud $\alpha \in O_n$, pak $\alpha \cup \{\alpha\}$ je nejmenší ordinální číslo větší než α.*

Důkaz. Nejprve ukážeme, že to je ordinální číslo. Protože je α tranzitivní, tak $\alpha \cup \{\alpha\}$ je taky tranzitivní (rozbor případů). Protože $\alpha \subseteq O_n$, tak dokonce je $\alpha \cup \{\alpha\}$ tranzitivní množina ordinálních čísel, podle posledního lemmatu je tedy také ordinálním číslem. Nyní, že je nejmenší. Je-li $\beta < \alpha \cup \{\alpha\}$, neboli $\beta \in \alpha \cup \{\alpha\}$, pak $\beta \in \alpha$ nebo $\beta = \alpha$, tedy $\beta \leq \alpha$.

❑

Definice 56. Je-li α ordinální číslo, tak ordinál $\alpha + 1 := \alpha \cup \{\alpha\}$ nazýváme následníkem α, a ordinál α nazýváme předchůdcem $\alpha + 1$.

Definice 57. Ordinální číslo α je izolované $\equiv$ $\alpha = 0$ nebo α má předchůdce. Jinak je α limitní.

Příklad. Každé $n \in \omega$ nebo $\omega + 1 = \omega \cup \{\omega\}$ jsou izolované, ale ω je limitní.

Věta 59 (Princip transfinitní indukce)**.** *Je-li $A \subseteq O_n$ třída t.ž. pro $\forall \alpha \in O_n$ platí*

$$\alpha \subseteq A \Rightarrow \alpha \in A,$$

potom $A = O_n$.

Důkaz. Pro spor nechť $O_n \setminus A$ není prázdná. Jelikož $(O_n, \leq)$ je dobře uspořádaná množina, tak existuje nejmenší prvek α této třídy. Protože α je nejmenší, tak každé $\beta \in \alpha$ musí být prvkem A. Tedy $\alpha \subseteq A$ a z předpokladu $\alpha \in A$, což je spor.

❑

Ekvivalentně lze P.T.I. formulovat zvlášť pro izolované a limitní ordinály. S touto formulací se pak lépe dokazují některá tvrzení.

Věta 60 (Princip transfinitní indukce II)**.** *Je-li $A \subseteq O_n$ třída splňující*

1. $0 \in A$,
2. $\alpha \in A \Rightarrow \alpha + 1 \in A$, *…tohle je přesně indukce pro přirozená čísla*
3. *je-li α limitní, pak $\alpha \subseteq A \Rightarrow \alpha \in A$,*

potom $A = O_n$.

Pomocí transfinitní indukcí dokazujeme vlastnosti různých nekonečných objektů. Transfinitní rekurze nám zase umožňuje konstruovat konstruujeme různé rekurzivně definované nekonečné objekty.

Věta 61 (O konstrukci transfinitní rekurzí)**.** *Je-li $G : V \to V$ třídové zobrazení, pak existuje právě jedno třídové zobrazení $F : O_n \to V$ splňující*

$$F(\alpha) = G(F[\alpha]).$$

Můžeme použít i jinou konstrukci, třeba $F(\alpha) = G(F \restriction \alpha)$. Zkrátka něco rekurentního.

Intuice. $F(0) = G(0)$, $F(1) = G(F[1]) = G(\{F[0]\})$, prostě už to mám pro všechna menší ordinální čísla a pomocí toho udělám to další. Umožňuje konstrukci funkcí definovaných rekurzivně. Například můžeme definovat $F_n(0) \coloneqq n$ a $F_n(S(m)) \coloneqq S(F_n(m))$.

Důkaz. Pomocí transfinitní indukce a axiomu nahrazení. ❑

Věta 62. *Axiom výběru $\Longrightarrow$ Well-ordering principle.*

Důkaz. Nechť A je množina, a g selektor na $\mathcal{P}(A)$. Pomocí transfinitní rekurze sestrojíme dobré uspořádání množiny A. Definujeme funkci $f(0) \coloneqq g(A)$, $f(\beta) \coloneqq g(A \setminus f[\beta])$, takže pro β si z A vyberu nějaký prvek, který jsem ještě nepoužil. Vlastně si prvky té množiny A očíslujeme, jako by to byla přirozená čísla. To je hlavní myšlenka toho důkazu. ❑

7.6 Aplikace konstrukce transfinitní rekurzí

Nejprve dva příklady na které rekurze není potřeba.

Příklad. $\mathbb{R}^3$ je sjednocením navzájem mimoběžných přímek.

Příklad. $\mathbb{R}^3$ je sjednocením navzájem disjunktních kružnic.

Tohle už bez rekurze (AoC) nejde, nebo na to alespoň zatím nikdo nepřišel.

Příklad. $\mathbb{R}^3$ je sjednocením navzájem disjunktních jednotkových kružnic.

Řešení. Pomocí AoC, W-O a transfinitní rekurze. Očíslujeme body $\mathbb{R}^3$ ordinálními čísly a dobře je uspořádáme jako $x_0, x_1, \dots x_\omega, x_{\omega+1}, \dots$, potom

$$\mathbb{R}^3 = \{x_\alpha \,|\, \alpha < 2^\omega\},$$

kde 2^ω je kardinální číslo t.ž. $2^\omega \approx \mathcal{P}(\omega) \approx \mathbb{R}$, t.j. nejmenší ordinální číslo s touto mohutností. Obecně když jsou κ,α kardinální čísla, tak $\alpha < \kappa \Rightarrow \alpha \prec \kappa$.

Vyrobíme soubor $\left\langle C_\alpha \mid \alpha < 2^\omega \right\rangle$ disjunktních jednotkových kružnic (nebo $\varnothing$, když ji nepotřebuji) tak, aby $\bigcup_{\alpha<2^\omega} C_\alpha = \mathbb{R}^3$. Stačí definovat C_α rekurzivně, známe-li $\{C_\beta \,|\, \beta < \alpha\}$. Pomocí C_α chci pokrýt bod x_α, pokud $x \in \bigcup_{\beta<\alpha} C_\beta$, potom $C_\alpha \coloneqq \varnothing$ (bod jsem již pokryl). Jinak C_β leží v méně než 2^ω nadrovinách (nejhorší případ: každá kružnice v jedné). Tedy existuje nadrovina H_α procházející x_α neobsahující žádnou kružnici $C_\beta, \beta < \alpha$. Kružnice ji ale mohou protínat ovšem vždy nejvýše ve dvou bodech, opět v nejhorším případě dva průsečíky, tedy množina průsečíků $\bigcup_{\beta<\alpha}(H_\alpha \cap C_\beta) \preceq 2 \times \alpha \prec 2^\alpha$. Chceme najít nějakou kružnici co leží v rovině H_α ale neprotíná žádný z těch průsečíků. Každý bod $x \in H_\alpha$ určuje nejvýše 2 jednotkové kružnice procházejících body x_α a x. Tedy počet zakázaných kružnic je maximálně $4 \times \alpha \prec 2^\omega$. Čili lze zvolit (pomocí AoC) C_α tak, že $x_\alpha \in C_\alpha$, $C_\alpha \subseteq H_\alpha$ a $C_\beta \cap C_\alpha = \varnothing$ pro $\beta < \alpha$. Použijeme selektor na $\mathcal{P}(\{C \,|\, C$ je jednotková kružnice v $R^3\})$. Nakonec

$$\bigcup_{\alpha<2^\omega} C_\alpha = \{x_\alpha \,|\, \alpha < 2^\omega\} = \mathbb{R}^3.$$

Příklad. V $\mathbb{R}^2$ existuje množina, která má s každou přímkou společné právě dva body. Hyperbola je k tomu docela blízko, ale ne úplně. Také vyžaduje rekurzi.

Zdroje

Tento text jsou převážně mé poznámky z předmětu NAIL063, vyučovaného na MFF UK doc. Kynčlem, web přednášky ZDE. Přednáška vychází z první a části druhé kapitoly [1]. Velmi hezké povídání o úvodu do teorie množin je také na webu matematického korespondenčního semináře [3]. V kapitole o logice jsem vycházel ze skript doktora Bulína [2].

[1] Bohuslav Balcar a Petr Štěpánek. *Teorie množin.* Vydání 2., opravené a rozšířené. Praha: Academia, 2001. ISBN: 80-200-0470-X.

[2] Jakub Bulín. *NAIL062 Výroková a predikátová logika: zápisky z přednášky.* 2023, s. 71–82. URL: `https://github.com/jbulin-mff-uk/nail062/raw/main/lecture/lecture-notes/lecture-notes.pdf` (cit. 10. 12. 2023).

[3] Matematický korespondenční seminář. *Do nekonečna a ještě dál.* URL: `https://prase.cz/archive/35/serial.pdf` (cit. 25. 12. 2023).